

Commission nationale de contrôle
des techniques de renseignement

CNCTR

4e Rapport d'activité 2019

SOMMAIRE

ANNEXES

Avant-propos

Le quatrième rapport annuel de la Commission nationale de contrôle des techniques de renseignement (CNCTR) permettra au lecteur d'avoir accès à des indications précises sur l'activité de contrôle de cette institution.

Alors que les rapports précédents insistaient sur le contrôle *a priori* des demandes de techniques de renseignement, la CNCTR donne cette année des précisions jusqu'à présent inédites sur son activité de contrôle *a posteriori* de la mise en œuvre des techniques de renseignement.

S'agissant du contrôle *a priori*, le lecteur aura accès aux mêmes informations que les années précédentes. Il pourra ainsi constater, à travers des données chiffrées, l'évolution depuis 2015 des finalités légales invoquées pour réaliser des surveillances et celle de l'utilisation de différentes techniques de renseignement.

Deux principaux constats peuvent à cet égard être dressés.

S'agissant en premier lieu des finalités, la prévention du terrorisme continue, depuis 2015, à fonder la plus grande partie des demandes de techniques de renseignement. La prévention de la criminalité organisée est la deuxième finalité la plus invoquée. La prévention des violences collectives a pris, depuis la fin de l'année 2018, une part plus importante qu'auparavant, l'invocation de cette finalité continuant cependant à faire l'objet d'une vigilance particulière de la CNCTR.

S'agissant en second lieu des techniques utilisées, leur nombre est globalement stable (+ 0,3 %) mais il recouvre des évolutions significatives, en hausse ou en baisse, selon les techniques.

Le calcul, établi par la CNCTR depuis 2016, du nombre des personnes surveillées au moyen de techniques de renseignement (22 210 en 2019), permet de constater une progression de 0,8 %, plus faible qu'en 2018. Cet indicateur confirme, en outre, les priorités des services en matière de prévention du terrorisme et de prévention de la criminalité et de la délinquance

organisées. Il permet de suivre, dans la durée, l'impact des activités de renseignement sur le droit au respect de la vie privée et d'observer son évolution.

Pour la première fois, le rapport donne des informations détaillées sur l'exercice du contrôle *a posteriori* de la commission. À travers les développements consacrés à cette thématique, le lecteur pourra ainsi se faire une idée plus précise des méthodes de contrôle utilisées, des constats établis sur la mise en œuvre des techniques de renseignement et plus globalement du respect par les services du cadre juridique. Il sera éclairé sur le rôle joué par le Groupement interministériel de contrôle (GIC), partenaire essentiel de la CNCTR dans son activité de contrôle. Il pourra également remarquer que la capacité de contrôle *a posteriori* de la CNCTR rencontre une limite tenant à l'impossibilité pour elle, en l'état actuel, d'accéder aux fichiers de souveraineté exploités par ces services. La CNCTR continuera, dans ses futurs rapports, à retracer de manière précise les types d'irrégularités qui auront pu être relevés.

Le rapport rappelle le cadre juridique en vigueur et décrit les évolutions intervenues en 2019. Le principal changement concerne le renseignement pénitentiaire. Le rapport rend compte de manière intelligible des modifications assez complexes intervenues à son égard.

Le rapport évoque enfin les perspectives d'évolution du cadre légal en 2020. La grave situation sanitaire qui prévaut à la date de finalisation du présent rapport risque cependant de reporter ces perspectives.

Un résumé du cadre juridique en vigueur

Le livre VIII du code de la sécurité intérieure, créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement et complété notamment par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, prévoit que les services de renseignement peuvent être autorisés à mettre en œuvre, pour des finalités limitativement énumérées, des techniques destinées à recueillir des renseignements. Chaque autorisation est accordée par le Premier ministre.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) s'assure que les techniques de renseignement sont mises en œuvre sur le territoire national conformément au cadre légal. Elle est consultée préalablement à la décision du Premier ministre sur toutes les demandes tendant à mettre en œuvre une technique ou, s'agissant de la surveillance des communications électroniques internationales, sur toutes les demandes tendant à exploiter des communications interceptées. La CNCTR vérifie également *a posteriori* que les prescriptions légales ont été respectées, en contrôlant l'exécution des autorisations accordées et en vérifiant qu'aucun recueil ou qu'aucune exploitation soumis à autorisation n'a été irrégulièrement mis en œuvre. Elle exerce un contrôle de légalité, qui inclut un contrôle de la proportionnalité des atteintes portées à la vie privée par rapport aux finalités poursuivies.

Les services de renseignement peuvent être des services spécialisés, dits du « premier cercle ». Ce sont :

- la direction générale de la sécurité extérieure (DGSE) ;
- la direction du renseignement et de la sécurité de la défense (DRSD) ;
- la direction du renseignement militaire (DRM) ;
- la direction générale de la sécurité intérieure (DGSI) ;
- le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) ;

- le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin).

D'autres services peuvent se voir confier des missions de renseignement. Ces services, dits du « second cercle », se trouvent notamment au sein de la direction générale de la police nationale, de la direction générale de la gendarmerie nationale, de la préfecture de police de Paris et de la direction de l'administration pénitentiaire.

En matière de surveillance intérieure, c'est-à-dire visant le territoire national, les techniques de renseignement pouvant être autorisées sont :

- **les accès administratifs aux données de connexion**[1], qui comprennent :
  - les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure),
  - les accès aux données de connexion en temps réel, à la seule fin de prévention du terrorisme (article L. 851-2 du code de la sécurité intérieure),
  - la mise en œuvre, à la seule fin de prévention du terrorisme, de traitements automatisés sur les seules données de connexion acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de services en ligne (article L. 851-3 du code de la sécurité intérieure),
  - la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure),
  - le balisage (article L. 851-5 du code de la sécurité intérieure),
  - le recueil de données de connexion par *IMSI catcher*[2] (article L. 851-6 du code de la sécurité intérieure) ;

---

1 - Définies à l'article L. 851-1 du code de la sécurité intérieure, les données de connexion sont les « *informations ou documents traités ou conservés par [les] réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ». Cette définition a été précisée par voie réglementaire à l'article R. 851-5 du code de la sécurité intérieure.

2 - Il s'agit de dispositifs techniques permettant de capter des données de connexion d'équipements terminaux, notamment le numéro de leur carte SIM ou *IMSI (international mobile subscriber identity)*.

- **les interceptions de sécurité, qui comprennent :**
  - l'interception, *via* le groupement interministériel de contrôle (GIC) ou par *IMSI catcher*, des communications acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de service en ligne (article L. 852-1 du code de la sécurité intérieure),
  - l'interception des communications échangées au sein d'un réseau privatif empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques (article L. 852-2 du code de la sécurité intérieure) ;
- **la captation de paroles prononcées à titre privé** (article L. 853-1 du code de la sécurité intérieure) ;
- **la captation d'images dans un lieu privé** (article L. 853-1 du code de la sécurité intérieure) ;
- **le recueil ou la captation de données informatiques** (article L. 853-2 du code de la sécurité intérieure) ;
- **l'introduction dans un lieu privé,** y compris à usage d'habitation (article L. 853-3 du code de la sécurité intérieure), qui ne constitue pas à proprement parler une technique de renseignement mais peut être autorisée, par décision spécifique, à la seule fin de mettre en place, utiliser ou retirer un dispositif de balisage, de captation de paroles, de captation d'images ainsi que de recueil ou de captation de données informatiques.

En matière de surveillance des communications électroniques internationales, l'interception de ces communications ainsi que différentes mesures d'exploitation portant sur des communications ou des seules données de connexion peuvent être autorisées (articles L. 854-1 et suivants du code de la sécurité intérieure).

Les finalités pouvant justifier la mise en œuvre des techniques de renseignement sont limitativement énumérées à l'article L. 811-3 du code de la sécurité intérieure :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
- les intérêts économiques, industriels et scientifiques majeurs de la France ;
- la prévention du terrorisme ;
- la prévention des atteintes à la forme républicaine des institutions, la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous et la prévention des violences collectives de nature à porter gravement atteinte à la paix publique ;
- la prévention de la criminalité et de la délinquance organisées ;
- la prévention de la prolifération des armes de destruction massive.

Le nouveau service du « second cercle » chargé du renseignement pénitentiaire peut en outre être autorisé à recourir à un nombre limité de techniques pour une finalité propre, prévue à l'article L. 855-1 du code de la sécurité intérieure, à savoir prévenir les évasions et assurer la sécurité au sein des établissements pénitentiaires.

Toute personne peut saisir la CNCTR d'une réclamation tendant à ce que la commission vérifie qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Une fois cette faculté de réclamation utilisée, la personne peut présenter une requête devant une formation spécialisée du Conseil d'État pour demander au juge administratif de mener des vérifications similaires.

Pour une description plus détaillée du cadre légal et de ses évolutions, le lecteur est invité à consulter le premier rapport d'activité 2015/2016 de la CNCTR ainsi qu'à se rapporter aux premières parties des rapports suivants.

La composition de la CNCTR

Au cours de l'année 2019, le collège de la CNCTR était composé des neufs membres suivants :

- monsieur Francis DELON, conseiller d'État honoraire, président ;
- madame Catherine DI FOLCO, sénatrice du Rhône ;
- monsieur Michel BOUTANT, sénateur de la Charente ;
- madame Constance LE GRIP, députée des Hauts-de-Seine ;
- monsieur Jean-Michel CLÉMENT, député de la Vienne ;
- madame Martine JODEAU, conseillère d'État honoraire ;
- madame Christine PÉNICHON, avocate générale à la Cour de cassation ;
- monsieur Gérard POIROTTE, conseiller honoraire à la Cour de cassation ;
- monsieur Patrick PUGES, personnalité qualifiée en matière de communications électroniques.

Le secrétariat général de la CNCTR se composait, cette même année, d'un secrétaire général, d'un conseiller placé auprès du président de la commission, de onze chargés de mission et de quatre agents exerçant des fonctions de soutien.



Compte-rendu de l'activité de la CNCTR

1. Les modifications du cadre juridique en 2019 et ses perspectives d'évolution : la CNCTR attentive au maintien de la cohérence générale du corpus normatif

1.1 Les modifications du cadre juridique en 2019 : un renforcement des attributions des services du « second cercle »

1.1.1 L'adaptation des capacités du renseignement pénitentiaire motivée par des besoins opérationnels

Les dispositions législatives applicables aux techniques de renseignement, codifiées au livre VIII du code de la sécurité intérieure, ont connu plusieurs modifications depuis leur entrée en vigueur en 2015. Celles intervenues entre 2016 et 2018 ont été analysées dans les précédents rapports d'activité de la CNCTR[3].

Une nouvelle modification – la septième – est intervenue en 2019. Elle concerne le renseignement pénitentiaire et a été apportée par la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice[4].

On rappellera que la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement avait ouvert au Gouvernement la possibilité d'inclure des services du ministère de la justice

3 - Voir notamment les points 2.1.3 et 2.1.4.1 du premier rapport d'activité 2015/2016 de la CNCTR ainsi que les points 1.2, 1.4 et 1.6 du deuxième rapport d'activité 2017 et le point 1.1 du troisième rapport d'activité 2018.

4 - Cette loi sera désormais mentionnée comme la loi du 23 mars 2019.

dans le « second cercle » des services de renseignement[5]. Cette loi avait modifié l'article L. 811-4 du code de la sécurité intérieure pour prévoir que ces services pourraient être autorisés à recourir à des techniques de renseignement. Le décret n° 2017-36 du 16 janvier 2017 pris pour l'application de cette loi précisait que les services concernés étaient le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire et que ceux-ci pouvaient demander l'autorisation de mettre en œuvre des techniques de renseignement pour les finalités de prévention du terrorisme et de la criminalité et de la délinquance organisées, respectivement prévues au 4° et au 6° de l'article L. 811-3 du code de la sécurité intérieure. Il dressait en outre la liste des techniques auxquelles ces services pouvaient être autorisés à recourir[6].

Parallèlement à la montée en puissance du renseignement pénitentiaire pour la prévention du terrorisme et de la criminalité et de la délinquance organisées, le Gouvernement avait souhaité renforcer la compétence de l'administration pénitentiaire dans le domaine de la sécurité et du bon ordre des lieux de détention. À cette fin, avait été prévue une nouvelle finalité, propre à l'environnement carcéral, pouvant justifier la mise en œuvre de techniques de renseignement prévues au livre VIII du code de la sécurité intérieure. Un nouveau dispositif, élaboré à cette fin en deux temps par la loi du 3 juin 2016 mentionnée précédemment puis par la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique[7] prévoyait que l'administration pénitentiaire était autorisée, pour prévenir les évasions et assurer la sécurité et le bon ordre des lieux de détention, à recourir à des techniques relevant, selon les cas, du code de procédure pénale (article 727-1 de ce code) ou du code de la sécurité intérieure. Un nouvel article L. 855-1 avait été inséré dans ce code à l'effet d'encadrer l'intervention dans ce domaine des services de renseignement pénitentiaire[8].

C'est ce second volet du cadre légal applicable au renseignement pénitentiaire qui a évolué en 2019.

5 - Voir le point 2.1.3 du premier rapport annuel 2015/2016 de la CNCTR.
6 - Voir le point 1.3.2 du rapport annuel 2017 de la CNCTR.
7 - Cette loi sera désormais mentionnée comme la loi du 28 février 2017.
8 - Voir, sur le détail du dispositif, le point 1.3.2 du deuxième rapport d'activité 2017 de la CNCTR.

1.1.1.1 La redéfinition du périmètre d’action des services du ministère de la justice chargés du renseignement pénitentiaire aux fins de prévenir les évasions et maintenir la sécurité des établissements pénitentiaires

Dans sa rédaction initiale issue de la loi du 28 février 2017, l’article L. 855-1 du code de la sécurité intérieure prévoyait que les services du ministère de la justice chargés du renseignement pénitentiaire pouvaient, à l’encontre des seules personnes détenues, être autorisés à accéder à des données de connexion en temps différé (article L. 851-1 du code), à géolocaliser des équipements terminaux en temps réel (article L. 851-4 du code), à baliser des objets (article L. 851-5 du code), à recueillir des données de connexion par *IMSI catcher* (article L. 851-6 du code) et à intercepter des correspondances *via* le GIC (I de l’article L. 852-1 du code) aux fins de prévenir les évasions et d’assurer la sécurité et le bon ordre au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

L’article 89 de la loi du 23 mars 2019 a renforcé la capacité des services chargés du renseignement pénitentiaire à recourir à des techniques de renseignement dans ce domaine, tout en précisant la finalité et le champ d’application de ces mesures de surveillance. Issues d’un amendement parlementaire[9], ces dispositions n’ont pas été formellement soumises à l’avis de la CNCTR.

Tout d’abord, la liste des techniques pouvant être mises en œuvre a été élargie, d’une part, aux interceptions de sécurité sur un réseau empruntant exclusivement la voie hertzienne (article L. 852-2 du code de la sécurité intérieure) et, d’autre part, aux captations de paroles prononcées à titre privé et aux captations d’images dans un lieu privé (article L. 853-1 du même code), y compris lorsque la mise en œuvre de ces captations nécessite l’introduction dans un lieu privé (article L. 853-3 de ce code).

9 - Cet article résulte en effet de l’adoption par l’Assemblée nationale, en première lecture, de l’amendement n°1132 présenté par la présidente de la commission des lois, madame Braun-Pivet, le 15 novembre 2018.

Ensuite, alors que la loi du 28 février 2017 limitait l'utilisation des techniques de renseignement à l'encontre des seules personnes détenues, les personnes surveillées peuvent désormais être autres que des détenus.

En contrepartie, cependant, ces nouvelles dispositions ont été assorties de garanties propres à limiter l'action des services du ministère de la justice chargés du renseignement pénitentiaire :

Premièrement, les finalités pouvant justifier le recours aux techniques de renseignement sont désormais limitées à la prévention des évasions et au maintien de la sécurité au sein des établissements pénitentiaires. Dans sa rédaction issue de la loi du 28 février 2017, l'article L. 855-1 du code de la sécurité intérieure autorisait les services de l'administration pénitentiaire à mettre en œuvre des techniques de surveillance destinées à « prévenir les évasions » et « assurer la sécurité et le bon ordre au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues ». La loi du 23 mars 2019 a voulu mieux circonscrire la mission de police administrative qu'elle confie aux services de l'administration pénitentiaire en la limitant à la prévention des évasions et à la sécurité des établissements. La notion peu précise de « bon ordre » dans ces établissements n'est donc plus retenue.

Deuxièmement, les personnes surveillées ne peuvent être que des personnes présentant un risque particulièrement élevé d'évasion ou dont le comportement constitue une menace d'une particulière gravité pour la sécurité au sein des établissements pénitentiaires. Mais seules les personnes détenues peuvent faire l'objet des techniques de captation d'images ou de paroles dans un lieu privé.

Troisièmement, la loi du 23 mars 2019 énonce un principe d'interdiction de surveillance des communications ou des entretiens entre une personne détenue et son avocat. On notera que la CNCTR mettait déjà en œuvre cette interdiction en se fondant sur les dispositions de l'article L. 821-7 du code de la sécurité intérieure selon lesquelles un avocat ne peut être l'objet d'une mesure de surveillance à raison de l'exercice de sa profession.

Quatrièmement, des contingents, fixés par le Premier ministre après avis de la CNCTR, limitent le nombre maximal d'autorisations simultanément en vigueur en ce qui concerne les interceptions de sécurité sur un réseau empruntant exclusivement la voie hertzienne, les captations de paroles prononcées à titre privé, les captations d'images dans un lieu privé et les introductions dans un lieu privé.

Au total, si le législateur a étendu les pouvoirs des services chargés du renseignement pénitentiaire dans un domaine ne relevant pas de la défense ou de la promotion des intérêts fondamentaux de la Nation prévus par l'article L. 811-3 du code de la sécurité intérieure, il a assorti cette extension de garanties permettant de concilier le droit au respect de la vie privée et l'impératif de sécurité dans les établissements pénitentiaires.

Saisi de quatre recours émanant de plus de soixante députés et de plus de soixante sénateurs, le Conseil constitutionnel a estimé que le législateur avait assorti les dispositions de l'article 89 de la loi du 23 mars 2019 « *de garanties propres à assurer une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée, l'inviolabilité du domicile et le secret des correspondances* » et les a déclarées conformes à la Constitution.

1.1.1.2 La création du Service national du renseignement pénitentiaire (SNRP)

Par un arrêté du 29 mai 2019[10], la garde des sceaux, ministre de la justice, a décidé la création d'un service à compétence nationale dénommé « Service national du renseignement pénitentiaire » (SNRP) en remplacement du bureau central du renseignement pénitentiaire et des échelons territoriaux correspondants.

10 - Voir l'arrêté du 29 mai 2019 portant création et organisation d'un service à compétence nationale dénommé « Service national du renseignement pénitentiaire ».

Bien qu'il poursuive les mêmes missions que son prédécesseur et s'appuie sur une organisation territoriale comparable, la création de ce nouveau service à compétence nationale nécessitait de substituer, dans la partie réglementaire du livre VIII du code de la sécurité intérieure, la mention du nouveau service à celle du bureau central du renseignement pénitentiaire et des échelons territoriaux correspondants. Cette substitution concernait aussi bien les missions rattachables au régime de droit commun applicable aux services de renseignement du « second cercle », prévu à l'article L. 811-4 du code de la sécurité intérieure, que le cadre propre au renseignement pénitentiaire, prévu à l'article L. 855-1 du même code aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires.

Le 23 mai 2019, la CNCTR a été saisie pour avis par la garde des sceaux, ministre de la justice, d'un projet de décret pris pour l'application de ces deux dispositions législatives.

a) Le projet de décret prévoyait que le SNRP, **en tant que service du « second cercle » relevant de l'article L. 811-4 du code de la sécurité intérieure**, soit autorisé à recourir aux mêmes techniques que son prédécesseur, c'est-à-dire aux techniques suivantes :
   - l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
   - la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
   - le balisage (article L. 851-5 du code de la sécurité intérieure) ;
   - le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
   - l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) ;
   - l'interception de correspondances par *IMSI catcher* (II de l'article L. 852-1 du code de la sécurité intérieure) ;
   - l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ;
   - la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;

- le recueil et la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé, y compris à usage d'habitation, pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images ou un dispositif de recueil ou de captation de données informatiques (article L. 853-3 du code de la sécurité intérieure).

Dans une délibération adoptée en formation plénière, le 4 juillet 2019[11], la CNCTR a émis un avis favorable à ce que le SNRP puisse être autorisé à mettre en œuvre l'ensemble des techniques énumérées ci-dessus, à l'exception de l'interception de correspondances par *IMSI catcher* prévue au II de l'article L. 852-1 du code de la sécurité intérieure.

Dans ses délibérations n° 3/2016 du 8 décembre 2016 et n° 2/2018 du 17 mai 2018, la CNCTR avait déjà relevé que la mise en œuvre de cette technique, encadrée de manière particulièrement restrictive par le II de l'article L. 852-1 du code de la sécurité intérieure, nécessitait un niveau d'expérience et de technicité très élevé. Le Gouvernement avait néanmoins maintenu, dans le décret, la possibilité pour les services chargés du renseignement pénitentiaire de solliciter la mise en œuvre d'interceptions de correspondances par *IMSI catcher*. Mais, jusqu'alors, la technique n'avait fait l'objet d'aucune demande émanant de ces services. Constatant que le niveau d'expérience et de technicité requis n'était toujours pas atteint au terme des deux premières années d'utilisation des techniques par les services du ministère de la justice chargés du renseignement pénitentiaire, la CNCTR a réitéré son avis défavorable à ce que le nouveau service soit autorisé à mettre en œuvre cette technique.

Dans le décret d'application[12], le Gouvernement a cependant maintenu la possibilité pour le SNRP de solliciter la mise en œuvre d'interceptions de correspondances par *IMSI catcher*.

11 - Voir la délibération CNCTR n° 2/2019 du 4 juillet 2019, publiée en annexe n° 2 au présent rapport et sur le site internet de la commission.

12 - Voir le décret n° 2019-1503 du 30 décembre 2019 modifiant diverses dispositions relatives au renseignement pénitentiaire.

Le projet de décret prévoyait aussi d'étendre la liste des finalités pouvant être invoquées par le SNRP pour solliciter une autorisation de mise en œuvre d'une technique de renseignement.

Jusqu'alors, les services du ministère de la justice chargés du renseignement pénitentiaire ne pouvaient demander cette autorisation qu'aux seules fins de prévenir le terrorisme ou la criminalité et la délinquance organisées, en application, respectivement, du 4° et du 6° de l'article L. 811-3 du code de la sécurité intérieure.

Le projet de décret soumis à la CNCTR prévoyait que le SNRP pourrait, en outre, invoquer la finalité prévue au 5° de l'article L.811-3 du code de la sécurité intérieure qui vise la prévention des atteintes à la forme républicaine des institutions (a), des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 (b) et des violences collectives de nature à porter gravement atteinte à la paix publique (c).

Après avoir rappelé, dans sa délibération du 4 juillet 2019, la particulière vigilance avec laquelle elle examine l'invocation de cette finalité, la CNCTR a estimé plausible le risque que des détenus organisent, favorisent ou coordonnent des actions violentes d'une gravité particulière depuis leur lieu de détention, fondant dès lors le besoin du SNRP de surveiller les communications électroniques des personnes détenues. En conséquence, elle a émis un avis favorable à ce que le SNRP sollicite, au titre de la finalité énoncée au 5° de l'article L. 811-3 du code de la sécurité intérieure, l'autorisation de mettre en œuvre les techniques suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) ;
- le recueil et la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure).

La CNCTR s'est, en revanche, prononcée défavorablement sur l'accès à toutes les autres techniques demandées[13] estimant que le besoin d'y recourir n'était pas avéré. Le Gouvernement a suivi l'avis de la commission.

Le projet de décret prévoyait par ailleurs que le SNRP pourrait être désormais autorisé à s'introduire dans des lieux d'habitation pour mettre en place, utiliser ou retirer des dispositifs de surveillance sur le fondement de la finalité prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure relative à la prévention de la criminalité et de la délinquance organisées[14].

La CNCTR a rappelé à cet égard qu'elle avait considéré, dans sa délibération n° 3/2016 du 8 décembre 2016[15], que la cellule de détention et les lieux assimilés, tels que les unités de vie familiale, devaient, parce qu'ils abritent une part essentielle de la vie privée des personnes détenues, être regardés comme des lieux d'habitation au sens de l'article L. 853-3 du code de la sécurité intérieure, nécessitant dès lors, pour la mise en œuvre de techniques, une demande d'autorisation spécifique d'introduction dans ce lieu d'habitation, examinée par la CNCTR en formation collégiale.

Compte tenu de ces garanties particulières, la CNCTR a émis un avis favorable à l'évolution proposée, sous réserve que les lieux d'habitation concernés soient uniquement des cellules de détention ou des lieux assimilés, tels que des unités de vie familiale.

Dans le décret d'application du 30 décembre 2019, le Gouvernement a suivi cette recommandation en autorisant la mise en œuvre de techniques nécessitant une introduction dans un lieu d'habitation « *à l'encontre des seules personnes détenues* ».

---

13 - Les autres techniques demandées étaient la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure), le balisage (article L. 851-5 du code), l'interception de correspondances par *IMSI catcher* (II de l'article L. 852-1 du code), l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code), la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code) et l'introduction dans un lieu privé, y compris à usage d'habitation, pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images ou un dispositif de recueil ou de captation de données informatiques (article L. 853-3 du code).

14 - Il est rappelé que les autres services du second cercle ne sont autorisés à accéder à des lieux d'habitation pour la mise en place, l'utilisation ou le retrait de dispositifs nécessaires à la mise en œuvre de certaines techniques de renseignement qu'au titre de la seule finalité de prévention du terrorisme.

15 - Délibération publiée en annexe n° 1 du deuxième rapport d'activité 2017 de la CNCTR et sur le site internet de la commission.

Le projet de décret prévoyait enfin de supprimer la restriction prévue au III de l'article R. 811-2 du code de la sécurité intérieure, en application de laquelle les services du ministère de la justice chargés du renseignement pénitentiaire peuvent mettre en œuvre des techniques « *pour le seul exercice des missions qui sont assignées à l'administration pénitentiaire envers les personnes qui lui sont confiées par l'autorité judiciaire en application de l'article 2 de la loi du 24 novembre 2009*[16] ».

La commission a estimé justifiés les besoins exprimés à cet égard dans la saisine et n'a pas émis d'objection à ce que le SNRP mette en œuvre des techniques de renseignement à l'encontre de personnes autres que détenues, sous les réserves énoncées précédemment.

Dans le décret du 30 décembre 2019, le Gouvernement a retiré la restriction aux personnes confiées à l'administration pénitentiaire par l'autorité judiciaire, mais a circonscrit l'activité du SNRP à « *un cadre d'action limité à l'enceinte des établissements pénitentiaires* ». Cette limitation à la prison du champ d'action territorial de ce service correspond à la vision que la CNCTR a préconisée depuis que les services chargés du renseignement pénitentiaire sont habilités à recourir à des techniques de renseignement.

b) **Au titre du régime propre au renseignement pénitentiaire prévu par l'article L. 855-1 du code de la sécurité intérieure**, le projet de décret avait pour seul objet d'actualiser la désignation du service du ministère de la justice placé sous l'autorité du directeur de l'administration pénitentiaire, autorisé à recourir à des techniques. Ces techniques sont en effet déjà mentionnées dans l'article L. 855-1, comme l'est aussi la finalité spécifique fondant ces dispositions[17].

16 - Il s'agit de la loi n° 2009-1436 du 24 novembre 2009 pénitentiaire.
17 - Voir les développements exposés au point 1.1.1 du présent rapport.

1.1.2 L'intégration de nouveaux services relevant du ministère de l'intérieur parmi les services de renseignement du « second cercle »

1.1.2.1 Des modifications liées à des réformes structurelles intervenues au sein de la direction centrale de la police judiciaire

a) La division de la sous-direction de la lutte contre la criminalité organisée et la délinquance financière en deux nouvelles entités : la sous-direction de la lutte contre la criminalité organisée (SDLCO) et la sous-direction de la lutte contre la criminalité financière (SDLCF)

Afin de renforcer le dispositif de lutte contre les formes complexes, organisées et transnationales de la criminalité financière et d'améliorer la coordination de ses services centraux, la direction générale de la police nationale (DGPN) a entrepris de modifier l'organisation de certains services placés sous son autorité, notamment au sein de la direction centrale de la police judiciaire (DCPJ).

Cette réforme a conduit à diviser la sous-direction de la lutte contre la criminalité organisée et la délinquance financière de cette direction centrale en deux sous-directions distinctes à compter du 1er juillet 2019[18].

Pour que ces nouvelles sous-directions puissent recourir à des techniques de renseignement, il était nécessaire qu'elles entrent dans le « second cercle » des services de renseignement et que leurs compétences en la matière soient précisées par un décret en Conseil d'État pris en application de l'article L. 811-4 du code de la sécurité intérieure.

Le 8 avril 2019, le ministre de l'intérieur a saisi la CNCTR pour avis d'un projet de décret en Conseil d'État désignant la sous-direction de la lutte

18 - Voir l'arrêté du ministre de l'intérieur en date du 19 avril 2019 modifiant l'arrêté du 5 août 2009 relatif aux missions et à l'organisation de la direction centrale de la police judiciaire.

contre la criminalité organisée (SDLCO) et la sous-direction de la lutte contre la criminalité financière (SDLCF) comme services de renseignement du « second cercle » et prévoyant les techniques de renseignement que pourraient être autorisées à mettre en œuvre ces nouvelles sous-directions ainsi que la finalité légale qu'elles pourraient invoquer.

La CNCTR a rendu son avis dans une délibération adoptée en formation plénière le 2 mai 2019[19].

La commission a constaté que les missions dévolues aux nouvelles sous-directions, de même que la liste des techniques de renseignement proposées et l'unique finalité invocable de prévention de la criminalité et de la délinquance organisées étaient identiques à celles de l'entité dont elles étaient issues. Elle a estimé que, plus de trois ans après l'entrée en vigueur du décret, adopté conformément aux recommandations formulées par la CNCTR dans ses délibérations n° 2/2015 du 12 novembre 2015 et n° 2/2018 du 17 mai 2018[20], permettant à la sous-direction de la lutte contre la criminalité organisée et la délinquance financière de mettre en œuvre des techniques de renseignement, aucun élément nouveau ne paraissait de nature à justifier un accès restreint ou modifié des nouvelles sous-directions aux techniques de renseignement autorisées pour l'entité dont elles étaient issues.

Elle a ainsi émis un avis favorable à ce que la SDLCO et la SDLCF puissent être autorisées à recourir aux techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;

19 - Voir la délibération de la CNCTR n° 1/2019 du 2 mai 2019, publiée en annexe n° 1 au présent rapport et sur le site internet de la commission.

20 - Ces délibérations sont annexées aux premier et troisième rapports d'activité de la CNCTR et sont disponibles sur le site internet de la commission.

- l’interception de sécurité exécutée auprès des opérateurs de communications électroniques *via* le groupement interministériel de contrôle (GIC) (I de l’article L. 852-1 du code de la sécurité intérieure) ;
- l’interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d’images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l’introduction dans un lieu privé ne constituant pas un lieu d’habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou un dispositif de captation d’images.

Le décret d’application n° 2019-684 du 28 juin 2019 a repris ces préconisations.

b) La création de l’Office anti-stupéfiants (OFAST) en remplacement de l’Office central pour la répression du trafic illégal de stupéfiants (OCRTIS).

Afin de renforcer le dispositif de lutte contre les trafics de stupéfiants en France, le ministre de l’intérieur a annoncé, au cours du mois de septembre 2019, le lancement d’un plan national de lutte contre les trafics de stupéfiants. Comprenant cinquante-cinq mesures, ce plan répond à six objectifs parmi lesquels l’approfondissement de la connaissance des trafics, l’intensification et la rationalisation des activités de terrain, l’accroissement de la lutte contre l’économie souterraine et les circuits de blanchiment du trafic de stupéfiants et l’amélioration des capacités des services.

Dans ce cadre, a été décidée la création d’un service à compétence nationale placé sous l’autorité directe du directeur central de la police judiciaire, dénommé office anti-stupéfiants (OFAST) et désigné comme chef de file en matière de lutte contre les trafics de drogues.

Ce nouveau service, chargé d’évaluer la menace représentée par les trafics de stupéfiants, a succédé à l’office central de répression du trafic illicite de stupéfiants le 1er janvier 2020. Il a une vocation opérationnelle tant dans la réalisation, sous la direction de l’autorité judiciaire, d’enquêtes menées en propre ou conjointement avec un service disposant de prérogatives de police judiciaire que dans l’apport d’une expertise.

La CNCTR a été saisie pour avis le 25 octobre 2019 par le ministre de l'intérieur d'un projet de décret désignant l'OFAST comme service de renseignement du « second cercle » et prévoyant les techniques de renseignements auxquelles ce service pourrait être autorisé à recourir ainsi que la finalité légale qu'il pourrait invoquer.

La CNCTR a rendu son avis dans sa délibération adoptée en formation plénière le 7 novembre 2019[21].

Bien que l'essentiel de l'activité opérationnelle de l'OFAST soit régie par les dispositions du code de procédure pénale, la commission a admis que, eu égard aux missions qui lui sont dévolues, ce service puisse avoir besoin de recueillir des renseignements à titre préventif et, dès lors, être désigné comme service de renseignement du « second cercle » susceptible de mettre en œuvre des techniques de renseignement limitativement énumérées par le pouvoir réglementaire.

Constatant que l'OFAST pourrait invoquer la même finalité de prévention de la délinquance et de la criminalité organisées que la sous-direction de la lutte contre la criminalité organisée et avoir recours aux mêmes techniques de renseignement, à l'exception des interceptions de correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne prévues par l'article L. 852-2 du code de la sécurité intérieure, la CNCTR n'a pas émis d'objection à ce que ce nouveau service puisse être autorisé à recourir aux techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;

21 - Voir la délibération de la CNCTR n° 5/2019 du 7 novembre 2019, publiée en annexe n° 5 au présent rapport et sur le site internet de la commission.

- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques *via* le GIC (article L. 852-1 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou un dispositif de captation d'images.

Le décret d'application n° 2019-1496 du 28 décembre 2019 reprend ces préconisations.

1.1.2.2 La réorganisation territoriale de la police nationale à Mayotte, en Guyane et en Nouvelle Calédonie

Les services déconcentrés de la police nationale à Mayotte, en Guyane et en Nouvelle Calédonie, autorisés à mettre en œuvre des techniques de renseignement pour certaines finalités prévues par la loi, en application du livre VIII du code de la sécurité intérieure[22], étaient jusqu'ici rattachés à plusieurs directions centrales au sein de la direction générale de la police nationale telles que celles de la sécurité publique ou de la police judiciaire.

Dans sa saisine du 25 octobre 2019 évoquée ci-dessus, le ministre de l'intérieur indiquait avoir décidé de les placer, à compter du 1er janvier 2020, à Mayotte, en Guyane et en Nouvelle Calédonie, sous l'autorité d'une direction territoriale de la police nationale, afin d'améliorer l'efficacité de la gouvernance territoriale et de rendre plus visible l'action unifiée de la police nationale dans des territoires confrontés à une forte délinquance et à des troubles à l'ordre public.

Le projet de décret soumis à l'examen de la commission visait à désigner les nouvelles directions territoriales de la police nationale comme services de

22 - Voir les dispositions réglementaires du livre VIII du code de la sécurité intérieure, dans leur rédaction résultant du décret n° 2015-1639 du 11 décembre 2015.

renseignement du « second cercle » et à prévoir que certains services déconcentrés placés sous leur autorité, en l'espèce les services du renseignement territorial et les antennes de police judiciaire, pourraient être autorisés à mettre en œuvre les techniques suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques *via* le GIC (article L. 852-1 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure), pour les seuls services du renseignement territorial ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise.

Les finalités susceptibles d'être invoquées étaient celles prévues aux 1°, 4°, 5° et 6° de l'article L. 811-3 du code de la sécurité intérieure.

Dans la délibération qu'elle a adoptée en formation plénière, le 7 novembre 2019, la CNCTR a relevé que les finalités et les techniques envisagées étaient les mêmes que celles dont les services déconcentrés concernés bénéficiaient déjà sous l'autorité de leur direction centrale. Ainsi, la création de directions territoriales de la police nationale n'apportait aucune modification aux compétences des services que les directions territoriales commanderaient de manière unifiée.

Près de quatre ans après l'entrée en vigueur du décret permettant aux services déconcentrés concernés d'être autorisés à mettre en œuvre des techniques de renseignement, aucun élément n'a conduit la CNCTR à recommander de restreindre ou de modifier leurs compétences en la matière. Elle a donc émis un avis favorable au projet de décret.

La nouvelle organisation territoriale a été entérinée par le décret d'application n° 2019-1496 du 28 décembre 2019 mentionné ci dessus.

1.1.2.3 Le rattachement de l'unité de coordination de la lutte antiterroriste (UCLAT) à la direction générale de la sécurité intérieure

Désignée comme un service de renseignement du « second cercle », l'unité de coordination de la lutte antiterroriste (UCLAT) avait jusqu'ici vocation à assurer une mission de coordination, d'animation et d'orientation des services de la police nationale en matière de lutte contre le terrorisme.

Dépourvue de rôle opérationnel, elle était uniquement autorisée à mettre en œuvre le recueil de données de connexion en temps différé prévu à l'article L. 851-1 du code de la sécurité intérieure, au titre des finalités de prévention du terrorisme, de prévention des atteintes à la forme républicaine des institutions et de prévention des actions tendant au maintien ou à la reconstitution de groupements dissous[23].

Dans sa saisine du 25 octobre 2019, évoquée ci-dessus, le ministre de l'intérieur faisait état de sa décision de rattacher l'UCLAT à la direction générale de la sécurité intérieure (DGSI) afin d'affirmer le rôle de chef de file de celle-ci en matière de lutte contre le terrorisme.

Dans la délibération qu'elle a adoptée en formation plénière le 7 novembre 2019, la CNCTR a pris acte de l'intégration de l'UCLAT dans un service spécialisé de renseignement dit du « premier cercle » pouvant être autorisé, en application du livre VIII du code de la sécurité intérieure, à mettre en œuvre toutes les techniques de renseignement au titre de toutes les finalités prévues par la loi. Ce rattachement, dont le décret n° 2019-1496 du 28 décembre 2019 a tiré les conséquences, n'a appelé aucune remarque de la part de la commission.

23 - Ces finalités sont celles prévues au 4° et aux a) et b) du 5° de l'article L. 811-3 du code de la sécurité intérieure.

1.1.3 Les techniques de renseignement soumises à contingentement : une progression raisonnée et équilibrée du nombre de techniques simultanément autorisées

Les techniques de renseignement soumises à contingentement

Jusqu'à l'entrée en vigueur de la loi du 23 mars 2019, trois techniques de renseignement étaient soumises au principe de contingentement, en application duquel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par décision du Premier ministre après avis de la CNCTR :

- les interceptions de sécurité (article L. 852-1 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du même code)[24] ;
- le recueil de données de connexion en temps réel (article L. 851-2 du même code).

Les contingents, surveillés quotidiennement par le GIC qui en informe la commission, sont conçus comme des incitations à ne recourir aux techniques concernées que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi* », ainsi que l'énonce l'article L. 801-1 du code de la sécurité intérieure.

24 - Le nombre d'appareils ou de dispositifs techniques pouvant être simultanément autorisés en application de l'article L. 851-6 du code de la sécurité intérieure a été fixé à 60 (35 pour le ministère de l'intérieur, 20 pour le ministère de la défense, 5 pour le ministère chargé des douanes) par un arrêté du Premier ministre en date du 15 janvier 2016 pris suivant les recommandations émises par la CNCTR dans une délibération adoptée en formation plénière le 18 décembre 2015. Ce contingent n'a, depuis, fait l'objet d'aucune demande de révision.

1.1.3.1 L’augmentation mesurée du contingent des interceptions de sécurité

Saisie par le Premier ministre le 15 mai 2019 d’un projet d’augmentation d’environ 11 % du contingent applicable aux interceptions de sécurité, précédemment fixé à 3 600 par une décision du 28 juin 2018, la CNCTR s’est prononcée par une délibération classifiée adoptée en formation plénière le 6 juin 2019. Après avoir constaté, comme lors des deux précédentes augmentations du contingent en 2017 et 2018, que le nombre maximal d’autorisations simultanément en vigueur était proche d’être atteint, elle a estimé avéré le besoin d’augmenter une nouvelle fois le contingent au regard notamment de la persistance, à un niveau élevé, de la menace terroriste.

Par une décision du 5 juillet 2019, le Premier ministre portait à 3 800 le nouveau contingent et le répartissait entre les différents ministères dont relèvent les services de renseignement.

Le tableau ci-dessous rappelle l’évolution du contingent des interceptions de sécurité depuis son inscription dans la loi en 1991.

	1991	1997	2003	2005	2009	2014	2015	2017	2018	2019
Intérieur	928	1 190	1 190	1 290	1 455	1 785	2 235	2 545	3 000	3 050
Défense	232	330	400	450	285	285	320	320	400	550
Douanes	20	20	80	100	100	120	145	145	150	150
Justice								30	50	50
TOTAL	1 180	1 540	1 670	1 840	1 840	2 190	2 700	3 040	3 600	3 800

1.1.3.2 Le contingent des recueils de données de connexion en temps réel : une progression adaptée aux besoins opérationnels des services

Si le recueil des données de connexion en temps réel est initialement apparu d'une faible utilité opérationnelle[25], sa redéfinition, issue de la loi du 30 octobre 2017[26], a renouvelé l'intérêt des services de renseignement pour cette technique désormais susceptible d'être mise en œuvre à l'encontre d'une personne appartenant à l'entourage d'un individu pouvant être porteur d'une menace justifiant la mise en œuvre de techniques de renseignement. Cette extension à l'entourage avait conduit le Conseil constitutionnel à soumettre la technique à un contingentement[27] afin d'opérer « *une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée* »[28].

Par une décision du Premier ministre en date du 8 janvier 2018 prise à la suite d'une délibération classifiée de la CNCTR adoptée en formation plénière le 7 décembre 2017, ce contingent avait été fixé à 500.

Saisie par le Premier ministre, le 18 octobre 2019, d'un projet portant à 720 le nombre d'autorisations de recueil de données de connexion en temps réel simultanément en vigueur, la CNCTR s'est prononcée par une délibération adoptée en formation plénière le 7 novembre 2019. Après avoir constaté que cette technique de renseignement, à laquelle il ne peut être recouru que pour la seule prévention du terrorisme, se révélait d'un intérêt opérationnel croissant pour les services et que le contingent en vigueur était presque atteint, la CNCTR a estimé avéré le besoin d'augmenter celui-ci au regard de la persistance, à un niveau élevé, de la menace terroriste[29].

Ce contingent a été fixé et réparti par une décision du Premier ministre en date du 25 novembre 2019.

25 - Voir le point 1.4 du deuxième rapport d'activité 2017 de la CNCTR.
26 - Il s'agit de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.
27 - Voir les dispositions du I bis de l'article L. 851-2 du code de la sécurité intérieure.
28 - Voir le paragraphe 11 de la décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017.
29 - Voir la délibération de la CNCTR n° 4/2019 du 7 novembre 2019, publiée en annexe n° 4 au présent rapport et sur le site internet de la commission.

Le tableau ci-dessous rappelle le contingent des recueils de données de connexion en temps réel depuis son instauration :

	2018	2019
Intérieur	430	650
Défense	50	50
Douanes	20	20
TOTAL	500	720

1.1.3.3 Les contingents prévus à l'article L. 855-1 du code de la sécurité intérieure : un juste équilibre entre protection de la vie privée et sécurité au sein des établissements pénitentiaires

L'article L. 855-1 du code de la sécurité intérieure autorise depuis 2017 les services du ministère de la justice chargés du renseignement pénitentiaire à recourir à certaines techniques de renseignement prévues au titre V du code de la sécurité intérieure aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires. La loi du 23 mars 2019 leur a donné accès, dans certaines conditions, à trois techniques supplémentaires : l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure), la captation de paroles prononcées à titre privé ou la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) et l'introduction dans un lieu privé pour y mettre en place, utiliser ou retirer des dispositifs de captation d'images ou de paroles (article L. 853-3 du code de la sécurité intérieure). L'accès à chacune de ces trois techniques est soumis à un contingentement[30] .

Saisie par le Premier ministre le 5 juillet 2019 d'un projet de décision fixant, pour chacune de ces trois techniques, un contingent d'autorisations égal à 20,

30 - Voir le point 1.1.1.1 du présent rapport.

la CNCTR s'est prononcée par une délibération adoptée en formation plénière le 10 juillet 2019[31].

Elle a considéré, en l'état des informations dont elle disposait sur les besoins opérationnels et les capacités techniques des services chargés du renseignement pénitentiaire, que les contingents envisagés n'étaient pas disproportionnés.

Chacun de ces trois contingents a été fixé à 20 par une décision du Premier ministre en date du 17 juillet 2019.

1.1.3.4 Le contingent applicable aux autorisations d'exploitation des communications internationales des personnes utilisant un identifiant technique rattachable au territoire national : une régulation à l'initiative de la CNCTR

Dans son troisième rapport d'activité pour l'année 2018[32], la CNCTR rendait compte des modifications apportées aux dispositions légales régissant la surveillance des communications électroniques internationales par la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

Ce texte a notamment introduit, au V de l'article L. 854-2 du code de la sécurité intérieure, une exception à l'interdiction d'utiliser des mesures de surveillance internationale pour assurer la surveillance individuelle d'une personne utilisant un identifiant technique rattachable au territoire français alors même que cette personne communique depuis la France. Il a prévu une nouvelle autorisation, réservée aux services spécialisés de renseignement dits du « premier cercle », d'exploitation des communications internationales d'une personne utilisant un identifiant technique rattachable au territoire national et qui communique depuis ce territoire[33]. Cette mesure de surveillance ne peut être autorisée que pour un nombre limité de finalités parmi celles énumérées à l'article L. 811-3 du code de la sécurité intérieure.

31 - Voir la délibération CNCTR n° 3/2019 du 10 juillet 2019, publiée en annexe n° 3 au présent rapport et sur le site internet de la commission.

32 - Voir le point 1.1.2 du troisième rapport d'activité 2018 de la CNCTR.

33 - Ces autorisations seront ci-après désignées par l'acronyme « AE-TN » communications.

Sont ainsi exclues, d'une part, la défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France et, d'autre part, la prévention des atteintes à la forme républicaine des institutions, la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous et la prévention des violences collectives de nature à porter gravement atteinte à la paix publique. Elle est également soumise à un contingentement qui limite, lorsqu'elle porte sur des correspondances, le nombre maximal d'autorisations d'exploitation simultanément en vigueur.

La CNCTR rappelle avoir été consultée par le Gouvernement sur le projet de modification législative ayant conduit à la création de cette nouvelle mesure de surveillance individuelle. Dans son avis rendu public en mai 2018[34], elle n'avait pas émis d'objection au principe de cette création mais elle avait estimé nécessaire de soumettre la mesure concernée, comme c'est déjà le cas pour les interceptions de sécurité, à un contingentement arrêté par le Premier ministre, après avis de la commission[35]. Cette préconisation avait alors été suivie par le Gouvernement.

Saisie par le Premier ministre le 15 janvier 2019 d'un projet fixant le nombre maximal d'autorisations simultanément en vigueur accordées sur le fondement du V de l'article L. 854-2 du code de la sécurité intérieure, la CNCTR s'est prononcée par une délibération classifiée adoptée en formation plénière le 7 février 2019. Elle a considéré que le contingent initialement proposé n'était pas suffisamment proportionné au regard des intérêts fondamentaux de la Nation susceptibles d'être invoqués pour recourir à cette mesure de surveillance individuelle et de l'atteinte que celle-ci porte au droit au respect de la vie privée. Elle a proposé de le limiter à 1 000.

34 - Voir la délibération CNCTR n° 1/2018 du 9 mai 2018, publiée en annexe n° 2 au troisième rapport d'activité 2018 de la CNCTR et sur le site internet de la commission.

35 - Ibid.

Par une décision du 19 avril 2019, le Premier ministre a suivi l'avis de la CNCTR. Il a fixé et réparti le contingent de la manière suivante :

	2019
Intérieur	750
Défense	210
Douanes	40
TOTAL	1000

Tableau récapitulatif des contingents en vigueur en 2019 par ministère et par technique

	Intérieur	Défense	Douanes	Justice	TOTAL
Recueils de données de connexion en temps réel *(article L. 851-2)*	650	50	20	-	720
Recueils de données de connexion par *IMSI catcher* *(article L. 851-6)*	35	20	5	-	60
Interceptions de sécurité *(I de l'article L. 852-1)*	3 050	550	150	50	3 800
« AE-TN » Communications	750	210	40	-	1 000
Interceptions de sécurité sur les réseaux exclusivement hertziens *(article L. 852-2)*	-	-	-	20*	-
Captations de paroles prononcées à titre privé ou captations d'images dans un lieu privé *(article L. 853-1)*	-	-	-	20*	-
Introductions dans un lieu privé *(article L. 853-3)*	-	-	-	20*	-

(*) contingents fixés en application des dispositions de l'article L. 855-1 du code de la sécurité intérieure dans leur rédaction issue de la loi du 23 mars 2019.

1.2 Les perspectives d'évolution du cadre juridique : des échéances en 2020

1.2.1 Un débat parlementaire prévu en 2020 sur le devenir d'une technique de renseignement

Le Parlement doit, en principe, débattre en 2020 du devenir de la technique de renseignement consistant à mettre en œuvre des algorithmes sur des données de connexion issues des réseaux des opérateurs de communications électroniques, à la seule fin de détecter des menaces terroristes.

Le recours à cette technique n'est actuellement autorisé que dans le cadre d'une expérimentation. L'article L. 851-3 du code de la sécurité intérieure, qui la prévoit, n'est en vigueur que jusqu'au 31 décembre 2020[36]. Avant cette date, le législateur devra donc, au vu notamment d'un rapport que le Gouvernement est tenu de lui présenter au plus tard le 30 juin 2020[37], décider s'il souhaite supprimer la technique, prolonger la période expérimentale ou pérenniser les dispositions concernées.

Ce débat au Parlement sur une question relevant du droit du renseignement pourrait, en outre, constituer une occasion pour faire un bilan plus général de l'application du cadre légal entré en vigueur en 2015. L'article 27 de la loi n° 2015-912 du 24 juillet 2015 a d'ailleurs prévu une évaluation de l'application des dispositions de cette loi par le Parlement dans un délai maximal de cinq ans après son entrée en vigueur.

36 - Initialement limitée au 31 décembre 2018 par l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, la validité de l'article L. 851-3 du code de la sécurité intérieure a été prolongée jusqu'au 31 décembre 2020 par l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

37 - Voir l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement dans sa rédaction résultant de l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

Dans son troisième rapport d'activité 2018, la CNCTR a émis des réflexions et formulé un certain nombre de propositions destinées à renforcer la cohérence du cadre juridique applicable au renseignement et à approfondir le contrôle sur le recueil et l'exploitation des données[38].

1.2.2 Des instances en cours devant les juridictions européennes, susceptibles de conduire à des évolutions du cadre légal

1.2.2.1 Des décisions attendues de la Cour de justice de l'Union européenne sur la question de la conservation des données de connexion

Dans un arrêt du 21 décembre 2016 dit Tele2 Sverige AB, la Cour de justice de l'Union européenne (CJUE) a jugé que le droit de l'Union[39] s'opposait à une « *réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* ».

Ce faisant, l'arrêt suscite des interrogations sur la conformité au droit de l'Union des législations des États membres qui imposent aux opérateurs de communications électroniques et aux fournisseurs de services en ligne de conserver, pendant une durée limitée, des données de connexion de tous leurs abonnés, dans l'hypothèse de leur éventuelle réquisition par l'autorité judiciaire ou par des services de renseignement. Eu égard aux difficultés qu'il pose, tant pour la conduite des enquêtes judiciaires que pour la recherche de renseignement, il a suscité plusieurs questions préjudicielles de juridictions nationales[40] invitant la CJUE à préciser voire reconsidérer sa position.

38 - Voir en particulier le point 1.2 du troisième rapport d'activité 2018 de la CNCTR.

39 - En l'espèce, la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, cette directive étant interprétée à la lumière des stipulations de la Charte des droits fondamentaux de l'Union européenne.

40 - La juridiction britannique chargée de contrôler les activités de renseignement et la Cour constitutionnelle belge ont respectivement posé à la CJUE des questions préjudicielles en ce sens les 31 octobre 2017 et 2 août 2018.

Le Conseil d'État a ainsi saisi la CJUE le 26 juillet 2018 de trois questions préjudicielles à l'occasion de deux recours dirigés contre plusieurs actes réglementaires applicables aux activités de renseignement. Ses questions ont porté sur les points suivants :

1°) L'obligation généralisée et indifférenciée imposée aux fournisseurs constitue-t-elle une ingérence justifiée par le « droit à la sûreté » garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne ?

2°) La directive du 12 juillet 2002 autorise-t-elle des mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés ?

3°) La directive du 12 juillet 2002 subordonne-t-elle la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ?

L'audience s'est tenue les 9 et 10 septembre 2019. Les conclusions de l'avocat général ont été rendues publiques le 15 janvier 2020[41]. Elles proposent notamment à la Cour de répondre au Conseil d'État que la directive du 12 juillet 2002 doit être interprétée en ce sens qu'elle :

1°) s'oppose à une réglementation nationale qui, même dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, impose aux opérateurs et aux prestataires de services de communications électroniques de conserver, de manière générale et indifférenciée, les données relatives au trafic et les données de localisation de tous les abonnés ainsi que les données permettant d'identifier les créateurs de contenus offerts par les fournisseurs de ces services ;

2°) s'oppose à une réglementation nationale qui n'instaure pas l'obligation d'informer les personnes concernées du traitement de leurs données à caractère personnel effectué par les autorités compétentes pour autant que cette communication ne compromette pas l'action de ces autorités ;

41 - Les conclusions sont communes aux trois renvois préjudiciels britannique, belge et français, examinés lors de la même audience des 9 et 10 septembre 2019.

3°) ne s'oppose pas à une réglementation nationale qui permet de recueillir en temps réel les données relatives au trafic et les données de localisation de personnes spécifiques, pour autant que ces actions soient menées conformément aux procédures prévues pour l'accès aux données à caractère personnel légalement conservées et avec les mêmes garanties.

L'arrêt de la CJUE est attendu dans les prochains mois.

Cet arrêt, et ce qu'en déduira le Conseil d'État, pourrait avoir des répercussions sur le dispositif légal en vigueur permettant aux services de renseignement d'accéder, s'ils y sont autorisés par le Premier ministre, après avis de la CNCTR, à des données de connexion conservées par les opérateurs de communications électroniques et concernant des personnes pouvant constituer une menace. Il pourrait aussi poser, pour d'autres techniques, la question de la mise en place d'une procédure d'information des personnes surveillées sur les mesures dont elles ont fait l'objet[42].

1.2.2.2 Deux instances en cours devant la Cour européenne des droits de l'Homme (CEDH) susceptibles d'avoir un impact sur le cadre légal des activités de renseignement

Dans un arrêt du 13 septembre 2018[43], la CEDH a examiné pour la première fois la compatibilité de dispositions légales régissant le partage international de données entre services de renseignement aux stipulations de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, en particulier le droit au respect de la vie privée. Il s'agissait en l'espèce du cadre légal britannique[44].

42 - Le lecteur pourra se reporter sur ce point à l'étude sur « la notification aux personnes concernées des mesures de surveillance mise en œuvre à leur encontre dans le passé », contenue dans le deuxième rapport d'activité 2017 de la CNCTR.

43 - Il s'agit de l'arrêt de la CEDH du 13 septembre 2018, n° 58170/13, affaire Big Brother Watch et autres contre Royaume-Uni, notamment les paragraphes 422 à 424.

44 - Après avoir observé que les services britanniques ne pouvaient exploiter de données transmises par des partenaires étrangers que sur le fondement d'une autorisation de droit interne, que cette transmission devait être proportionnée aux buts poursuivis, que les données ne pouvaient être conservées qu'aussi longtemps qu'elles étaient nécessaires à ces buts, enfin qu'un organe de contrôle indépendant, dénommé Investigatory Powers Commissioner's Office, se reconnaissait compétent pour contrôler les accords de partage international de renseignements, la CEDH a jugé que la législation britannique ne méconnaissait pas les stipulations de la Convention relatives au droit au respect de la vie privée.

Dans cette affaire, portant exclusivement sur les « flux entrants », la Cour a estimé que, comme pour tout dispositif permettant d'obtenir des renseignements, celui consistant à recevoir des données de partenaires étrangers devait avoir une base légale, accessible et prévisible, ainsi qu'être proportionné et contrôlable de manière adéquate. Elle a précisé que pourrait constituer une garantie adaptée le fait de subordonner l'exploitation de ces « flux » au respect des exigences légales applicables à la mise en œuvre de techniques de renseignement sur le territoire de l'État receveur et, qu'à tout le moins, la législation nationale devrait entourer de garanties la conservation, l'exploitation, la transmission et la destruction des données issues de ces échanges.

Cet arrêt de chambre n'est cependant pas définitif. Le 4 février 2019, le collège de la Grande chambre a en effet accepté la demande des requérants de lui renvoyer l'affaire. L'audience s'est tenue le 10 juillet 2019. L'arrêt de la Grande chambre devrait intervenir dans le courant de l'année 2020.

La CNCTR rappelle à cet égard qu'elle a, dans son troisième rapport d'activité 2018[45], suggéré d'entreprendre une réflexion sur l'encadrement des échanges de données entre les services de renseignement français et leurs partenaires étrangers.

Quatorze requêtes[46] ont par ailleurs été introduites devant la CEDH par des avocats et des journalistes contre la loi du 24 juillet 2015 relative au renseignement et sont toujours pendantes.

Sur le fondement des articles 8 et 10 combinés de la Convention, certains requérants soutiennent que les techniques de renseignement prévues par la loi ne satisfont pas aux exigences d'une base légale suffisante. Ils estiment ainsi que la notion d'« *informations ou documents* » pouvant être recueillis au moyen d'une technique de renseignement n'est pas définie et que la loi ne protège pas suffisamment les personnes exerçant la profession de journaliste ou d'avocat en ne prévoyant pas, selon eux, de règles garantissant, dans un cas, le secret des sources et, dans l'autre, celui des communications passées dans le cadre d'une activité de conseil.

45 - Voir le point 1.2.4 du troisième rapport d'activité 2018 de la CNCTR.

46 - Douze ont été introduites entre le 7 octobre et le 1er décembre 2015 puis deux ont été introduites le 21 avril 2017.

Ils estiment en outre que le législateur a retenu une définition large des finalités légales pouvant fonder la mise en œuvre de mesures de surveillance, le régime légal ainsi créé n'étant pas, selon eux, « *strictement nécessaire à la préservation des institutions démocratiques* ».

Sur le fondement de l'article 13 de la Convention, combiné avec les articles 8 et 10, les requérants se plaignent d'une insuffisance des garanties procédurales. Ils allèguent une absence de recours effectif en ce que, d'une part, le recours devant la CNCTR et le Conseil d'État ne remplit pas les exigences conventionnelles (méconnaissance des principes d'équité, du contradictoire et de l'égalité des armes) et, d'autre part, qu'il est impossible de saisir directement le Conseil d'État des mesures de surveillance internationale ou du recueil et d'exploitation d'informations venant de services étrangers.

L'arrêt de la Cour sur ces affaires devrait intervenir après celui rendu en Grande chambre dans l'affaire Big Brother Watch, sans qu'aucune indication précise de calendrier ne soit disponible à la date de publication de ce rapport. En l'état actuel de la jurisprudence de la Cour en matière de renseignement[47], il est délicat d'émettre des hypothèses sur l'issue de ces requêtes.

47 - Pour une analyse plus détaillée de cette jurisprudence, le lecteur peut consulter l'étude consacrée aux « Éléments de jurisprudence européenne sur le droit au respect de la vie privée en matière de renseignement » publiée dans le troisième rapport d'activité 2018 de la CNCTR.

2. Le contrôle de la mise en œuvre des techniques de renseignement : un contrôle *a priori* fondé sur un examen attentif des motifs invoqués, qui s'applique à toutes les demandes formulées par les services de renseignement

Aux termes de l'article L. 833-1 du code de la sécurité intérieure, la CNCTR veille à ce que les techniques de renseignement soient mises en œuvre sur le territoire national conformément au cadre légal qui les régit. Cette mission de contrôle porte également sur les mesures de surveillance des communications électroniques internationales, en application de l'article L. 854-9 du code de la sécurité intérieure.

Le contrôle préalable de la CNCTR a porté en 2019 sur un volume de demandes tendant à la mise en œuvre de techniques de renseignement comparable à celui constaté en 2018. Il s'est, en 2019 comme durant les années 2016, 2017 et 2018, exercé sur l'intégralité des demandes formulées par les services. Aucune demande n'a en effet été présentée selon la procédure d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure, qui dispense le Premier ministre, dans des cas exceptionnels, de consulter la CNCTR avant d'autoriser la mise en œuvre de certaines techniques.

Les moyens financiers et humains de la CNCTR

Composée d'un collège de neuf membres qui s'appuie sur un secrétariat général de dix-sept agents, la CNCTR dispose d'un budget propre qu'elle gère en toute indépendance.

Les crédits alloués par le Parlement à la CNCTR sont inscrits au budget général de l'État (mission « Direction de l'action du Gouvernement », programme n° 308 « Protection des droits et libertés », action n° 12 « Commission nationale de contrôle des techniques de renseignement »).

La loi de finances initiale pour 2019[48] a attribué à la CNCTR des montants de 2,5 millions d'euros pour ses dépenses de personnel et de 370 000 euros pour ses dépenses de fonctionnement. Comme en 2018, ces crédits ont été presque entièrement consommés.

Les dépenses de fonctionnement ont directement participé à l'accomplissement des activités de contrôle de la CNCTR. Elles ont couvert les frais de déplacement des membres et des agents pour contrôler des services de renseignement sur l'ensemble du territoire national. Elles ont financé l'achat et la maintenance des matériels informatiques constituant le réseau interne sécurisé de la commission. Enfin elles ont contribué à la sécurisation des locaux de la CNCTR qui, en tant que lieu abritant des informations et supports classifiés, doivent répondre aux normes de sécurité définies dans l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

48 - Voir la loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019.

2.1 Des évolutions selon les techniques de renseignement et les finalités invoquées

Comme dans ses trois premiers rapports d'activité, la CNCTR présente des éléments statistiques sur les techniques de renseignement relevant de la surveillance intérieure, c'est-à-dire destinées à surveiller des personnes situées sur le territoire national[49].

La CNCTR présente également, comme elle l'a fait pour la première fois dans son rapport d'activité de l'année 2018, le nombre d'avis *a priori* rendus en 2019 sur des demandes relevant de la surveillance des communications électroniques internationales.

Les éléments statistiques figurant dans le présent rapport sont le produit d'un travail d'extraction et d'agrégation de données mené par la CNCTR conjointement avec le GIC, puis de fiabilisation des résultats.

2.1.1 Le nombre d'avis préalables rendus par la CNCTR en matière de surveillance intérieure : des évolutions toujours contrastées selon les techniques de renseignement

En matière de surveillance intérieure, les avis préalables rendus par la CNCTR se répartissent comme indiqué dans le tableau général ci-dessous.

Les chiffres indiqués dans ce tableau incluent l'ensemble des demandes formées par les services de renseignement en 2016, 2017, 2018 et 2019.

49 - Voir le résumé du cadre juridique en vigueur en introduction au présent rapport.

	2016	2017	2018	2019	Évolution 2018/ 2019
Accès aux données de connexion en temps différé (identifications d'abonnés ou recensements de numéros d'abonnement) *(article L. 851-1 du code de la sécurité intérieure)*	32 096	30 116	28 741	25 051	-12,8 %
Accès aux données de connexion en temps différé (autres demandes, dont celles de « factures détaillées »[50]) *(article L. 851-1 du code de la sécurité intérieure)*	15 021	18 512	17 443	14 568	-16,5 %
Géolocalisations en temps réel *(article L. 851-4 du code de la sécurité intérieure)*	2 426	3 751	5 191	7 601	+46,4 %
Interceptions de sécurité *via* le GIC *(I de l'article L. 852-1 du code de la sécurité intérieure)*	8 137	8 758	10 562	12 574	+19 %
Autres techniques de renseignement [51]	9 408	9 295	11 361	13 749	+21 %
Ensemble des techniques de renseignement	67 088	70 432	73 298	73 543	+0,3 %

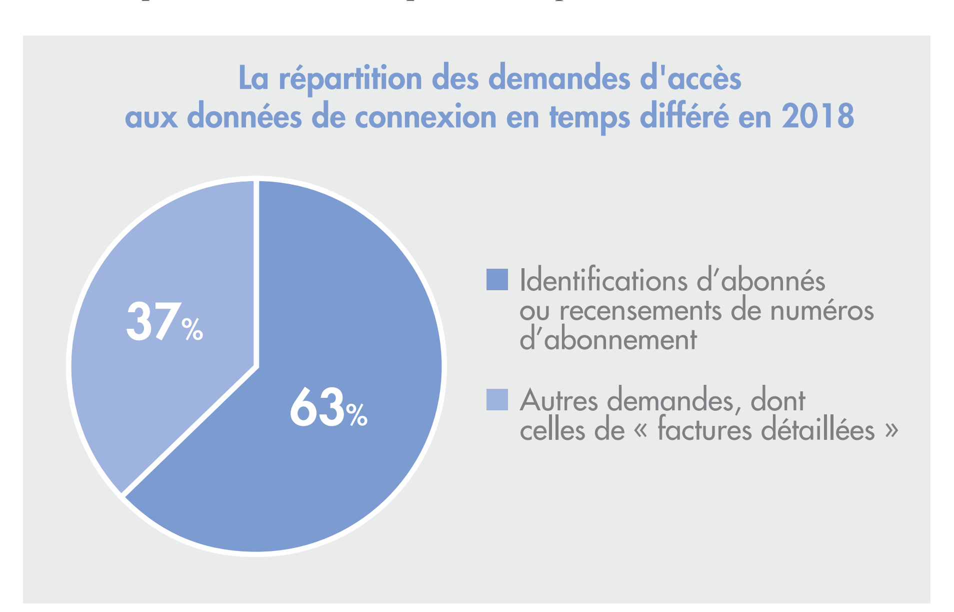
50 - Il s'agit d'obtenir la liste des communications d'une personne, ce qui peut révéler la date, la durée, le lieu de ces communications ainsi que le numéro ou l'identifiant technique du correspondant.

51 - Sont incluses les demandes d'accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure), celles de mise en œuvre de traitements automatisés sur des données de connexion (article L. 851-3 du même code), celles de balisage (article L. 851-5 du même code), celles de recueil de données de connexion par IMSI catcher (article L. 851-6 du même code), celles d'interception de sécurité par *IMSI catcher* (II de l'article L. 852-1 du même code), celles d'interception de sécurité sur un réseau empruntant exclusivement la voie hertzienne (article L. 852-2 du même code), celles de captation de paroles prononcées à titre privé ou celles de captation d'images dans un lieu privé (article L. 853-1 du même code), celles de recueil et de captation de données informatiques (article L. 853-2 du même code) et celles d'introduction dans un lieu privé (article L. 853-3 du même code).

Le tableau ci-dessus fait apparaître que le nombre total de demandes tendant à la mise en œuvre de techniques de renseignement en 2019 est stable (+ 0,3 %) par rapport à 2018. Ce résultat global recouvre cependant des évolutions contrastées selon les différentes techniques de renseignement.

Les demandes d'**accès aux données de connexion en temps différé** (article L. 851-1 du code de la sécurité intérieure), technique de renseignement la plus utilisée tout en étant la moins intrusive de celles prévues au livre VIII du code de la sécurité intérieure, ont connu une baisse de plus de 14 % en 2019.

Il est rappelé qu'en application de la méthode de comptabilisation de la CNCTR, une demande présentée au titre de l'article L. 851-1 du code de la sécurité intérieure est susceptible de porter sur plusieurs accès à la fois. Par exemple, une demande de recensement de numéros d'abonnement téléphonique d'une personne peut entraîner le recueil de plusieurs numéros auprès de plusieurs opérateurs de communications électroniques. Chaque demande peut donc conduire à plusieurs réquisitions.



Les demandes de **géolocalisation en temps réel** (article L. 851-4 du code de la sécurité intérieure) ont poursuivi en 2019 leur très forte progression. L'augmentation de plus de 46 % en 2019 est encore supérieure à celle observée en 2018.

Le recours aux **interceptions de sécurité** *via* le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) a encore crû de façon significative en 2019. Le taux d'augmentation s'élève à 19 %. Par comparaison, il était déjà de 20 % en 2018.

Les demandes portant sur les **autres techniques de renseignement** prévues aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure ont également nettement augmenté en 2019. Cette hausse de 21 %, presque identique à celle observée en 2018, confirme l'intérêt porté par les services à ces techniques complexes pour la collecte de renseignements qui ne peuvent, pour la plupart, être recueillis par un autre moyen légalement autorisé. Elle manifeste également une appropriation croissante de la maîtrise de ces techniques. Comme dans ses précédents rapports d'activité, la CNCTR a fait le choix d'indiquer le nombre de ces demandes de façon consolidée afin de respecter les dispositions de l'article L. 833-9 du code de la sécurité intérieure, qui prévoit que le rapport d'activité de la commission ne peut contenir d'informations couvertes par le secret de la défense nationale ni révéler des procédures ou des méthodes opérationnelles des services de renseignement.

S'agissant enfin de l'**algorithme**[52] sur des données de connexion en vue de détecter des menaces terroristes, aucune nouvelle autorisation de mise en œuvre n'a été sollicitée en 2019. À la fin de l'année 2019 trois algorithmes avaient été autorisés depuis l'entrée en vigueur du cadre légal et continuaient à être en fonctionnement.

52 - Il s'agit de la technique prévue par les dispositions de l'article L. 851-3 du code de la sécurité intérieure.

Les avis défavorables rendus par la CNCTR

En 2019, la CNCTR a rendu, hors demandes d'accès aux données de connexion en temps différé prévues à l'article L. 851-1 du code de la sécurité intérieure, 460 avis défavorables, soit 1,4 % du nombre d'avis rendus.

Ce taux, en constante diminution depuis 2015, est en cohérence avec les efforts déployés par les services de renseignement pour se conformer à l'ensemble des exigences imposées par le cadre juridique en vigueur et à la doctrine de mise en œuvre élaborée par la CNCTR.

Cette évolution constitue pour la CNCTR un indicateur de la qualité et de l'utilité du dialogue régulier qu'elle entretient avec les services demandeurs sur la mise en œuvre du cadre légal.

La CNCTR a, en outre, rendu 78 avis défavorables sur les demandes d'accès aux données de connexion en temps différé, soit environ 0,2 % du nombre d'avis rendus sur les demandes concernant cette technique.

Comme les années précédentes, le Premier ministre n'a, en 2019, accordé aucune autorisation après un avis défavorable de la commission. Les avis défavorables de la CNCTR ont ainsi toujours été suivis par le Premier ministre depuis l'entrée en vigueur du cadre légal, le 3 octobre 2015.

2.1.2 Les finalités invoquées dans les demandes de techniques de renseignement relevant de la surveillance intérieure : prépondérance constante de la prévention du terrorisme et renforcement de la prévention des violences collectives de nature à porter gravement atteinte à la paix publique

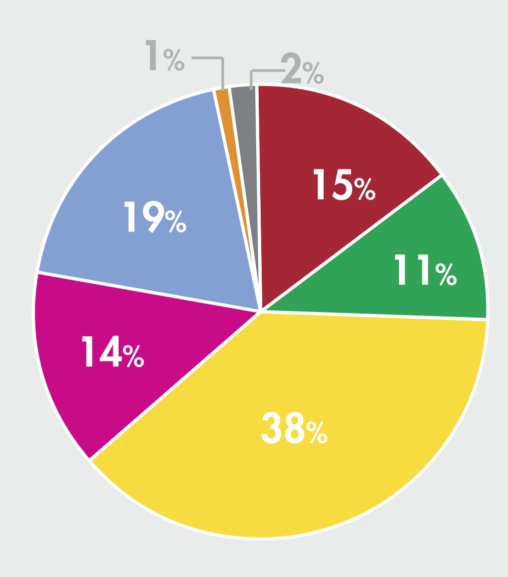
Les techniques de renseignement ne peuvent être mises en œuvre que pour la défense ou la promotion d'une liste limitative d'intérêts fondamentaux de la Nation énoncés à l'article L. 811-3 du code de la sécurité intérieure.

Conformément à la présentation retenue dans ses précédents rapports d'activité, la commission indique, pour l'ensemble des demandes tendant à la mise en œuvre de techniques de renseignement, la proportion de chacune des sept finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure.

Par ailleurs, et comme la commission l'a rappelé dans son rapport d'activité de l'année 2018, le service de renseignement du « second cercle » relevant du ministère de la justice et chargé du renseignement pénitentiaire peut, en application de l'article L. 855-1 du code de la sécurité intérieure, recourir également à une liste limitative de techniques pour des finalités qui lui sont propres, à savoir la prévention des évasions et le maintien de la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues[53]. En 2019, ces finalités ont été invoquées dans 0,08 % des demandes de techniques de renseignement. Dès lors qu'elles ne concernent qu'un seul service et qu'elles continuent à ce jour d'avoir un poids marginal, les deux finalités propres au renseignement pénitentiaire ne figurent pas dans le diagramme ci-dessous.

53 - Voir, pour une description des modifications légales ayant concerné ce service au cours de l'année 2019, le point 1.1.1 du présent rapport.

Les finalités fondant toutes les techniques de renseignement en 2019



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

La prévention du terrorisme, dont le premier rapport d'activité de la CNCTR avait montré qu'elle était devenue en janvier 2015 le fondement légal le plus invoqué à l'appui des demandes d'interceptions de sécurité, est demeurée les années suivantes très nettement prédominante lorsque l'on considère les demandes portant sur l'ensemble des techniques de renseignement. En dépit d'un léger déclin, cette finalité a encore motivé plus de 38 % des demandes soumises à la CNCTR en 2019.

Suivent en deuxième position, invoqués chacun dans des proportions comparables, d'une part la prévention de la criminalité et de la délinquance organisées (19 %), d'autre part le groupe de finalités relevant des intérêts géostratégiques de la France (18 %) (indépendance et défense nationales, intérêts majeurs de la politique étrangère de la France et prévention de l'ingérence étrangère, lutte contre la prolifération des armes de destruction massive). Ces taux connaissent peu de variations d'une année sur l'autre. Par comparaison, ils étaient respectivement de 17 % et 20 % en 2018.

En troisième et dernière position, viennent deux finalités dont l'importance relative est atténuée par le contexte sécuritaire et international mais qui motivent une partie significative de l'activité des services de renseignement. Il s'agit, d'un côté, de la défense et de la promotion des intérêts économiques, industriels et scientifiques majeurs de la France (11 %) et, de l'autre, de la prévention d'activités particulièrement déstabilisatrices de l'ordre public telles que les violences collectives de nature à porter gravement atteinte à la paix publique (14 %). Cette dernière finalité a connu une forte progression au cours des deux dernières années, passant de 6 à 9 % en 2018 puis de 9 à 14 % en 2019. La CNCTR rappelle qu'elle se montre particulièrement vigilante sur les demandes fondées sur cette finalité, considérant que la prévention de violences collectives ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, même extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.

2.1.3 Le nombre de personnes surveillées au moyen de techniques de renseignement relevant de la surveillance intérieure : une stabilité cohérente avec celle des demandes d'autorisation de mise en œuvre de techniques de renseignement

La CNCTR a repris, comme chaque année, l'indicateur qu'elle avait créé à l'occasion de son premier rapport d'activité[54] et a calculé le nombre de personnes ayant fait l'objet, en 2018, d'au moins une technique de renseignement prévue aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure. Comme les années précédentes, ce chiffre ne comprend pas les accès aux données de connexion en temps différé mentionnés au deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, c'est-à-dire les identifications d'abonnés ou les recensements de numéros d'abonnement[55].

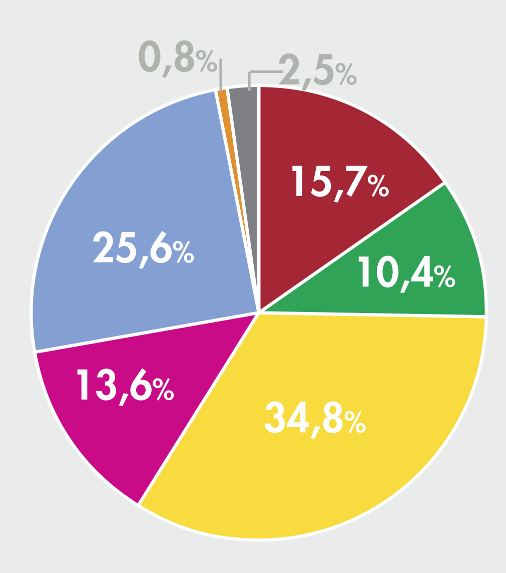
Les éléments de calcul utilisés comportent une marge d'erreur, évaluée à moins de 10 %, dès lors que les demandes tendant à la mise en œuvre de techniques de renseignement sont présentées par technique et non par personne, que le traitement informatisé des demandes n'a pas encore été entièrement harmonisé et, enfin, que certaines personnes faisant l'objet de surveillance ne sont pas nommément identifiées. Cependant, grâce aux développements informatiques conduits par le GIC et à l'amélioration des outils conçus par la commission lors de sa première année de fonctionnement, la fiabilité du calcul a été renforcée.

54 - Voir le point 3.3 du premier rapport d'activité 2015/2016 de la CNCTR.

55 - La CNCTR considère en effet que les identifications d'abonnés et les recensements de numéros d'abonnement constituent moins une mesure de surveillance à proprement parler qu'un acte préparatoire à des mesures de surveillance. De telles mesures commencent, pour la CNCTR, dès l'obtention de « factures détaillées » de la personne concernée en application du même article L. 851-1 du code de la sécurité intérieure.

	2016	2017	2018	2019	Évolution 2018/ 2019
Nombre de personnes surveillées	20 360	21 386	22 038	22 210	+ 0,8 %
Dont, au titre de la **prévention du terrorisme**	9 475 (46,5 % du total)	9 157 (42,8 % du total)	8 574 (38,9 % du total)	7 736 (34,8 % du total)	- 9,8 %
Dont, au titre de la **prévention de la criminalité et de la délinquance organisées**	4 969 (24,4 % du total)	5 528 (25,8 % du total)	5 416 (24,6 % du total)	5 693 (25,6 % du total)	+ 5,1 %

La répartition des personnes surveillées selon les finalités motivant leur surveillance en 2019



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

Le nombre de personnes surveillées progresse de 0,8 % entre 2018 et 2019. Cette relative stabilité est cohérente avec l'évolution globale de 0,3 % des demandes de techniques de renseignement.

De manière également cohérente avec le diagramme indiquant la répartition des finalités invoquées dans les demandes de techniques de renseignement, la proportion de personnes surveillées au titre de la prévention du terrorisme, qui s'élève à près de 35 % en 2019, est, bien qu'en légère baisse, nettement majoritaire, devant les quelque 26 % de personnes surveillées au titre de la prévention de la criminalité et de la délinquance organisées. On observe, par ailleurs, une progression par rapport à 2018 de la proportion de personnes surveillées sur le fondement de la prévention des violences collectives (de 9,6 à 13,6 %).

2.1.4 Le nombre d'avis préalables rendus par la CNCTR au titre de la surveillance internationale : une augmentation due pour l'essentiel à la modification législative intervenue en 2018

La CNCTR rend public, comme elle l'a fait l'année précédente[56], le nombre de demandes d'autorisation en matière de surveillance des communications électroniques internationales sur lesquelles elle s'est prononcée en 2019.

Les autorisations d'exploitation de communications internationales interceptées prévues au III de l'article L. 854-2 du code de la sécurité intérieure peuvent concerner les communications émises ou reçues au sein d'une zone géographique, par une organisation, par un groupe de personnes ou par une seule personne. L'autorisation prévue, depuis l'entrée en vigueur de la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, au V du même article ne peut quant à elle concerner

56 - Voir le point 2.1.4 du troisième rapport d'activité 2018 de la CNCTR. Pour mémoire, depuis l'entrée en vigueur de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, la consultation préalable de la commission sur les demandes d'exploitation de communications internationales interceptées, prévues au III et V de l'article L. 854-2 du code de la sécurité intérieure, est obligatoire.

qu'une seule personne et permet l'exploitation de ses communications utilisant un identifiant technique rattachable au territoire national, y compris lorsque la personne l'utilise pour communiquer depuis la France. Quelle que soit leur nature, ces autorisations d'exploitation ne peuvent être fondées que sur les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure.

En 2019, la commission a rendu 2 133 avis sur des demandes tendant à l'exploitation de communications internationales interceptées, contre 971 en 2018. Cette forte hausse s'explique par deux motifs. Le premier correspond à une modification de la pratique des services demandeurs, préconisée par la CNCTR, consistant à solliciter des autorisations d'exploitation plus circonscrites et plus précises. Elle conduit, corrélativement, à une augmentation du nombre de demandes d'autorisation soumises à l'examen de la commission, sans que cela corresponde à une extension du champ de la surveillance. Le second et principal motif d'augmentation du nombre des demandes est lié à l'entrée en vigueur des dispositions du V de l'article L. 854-2 du code de la sécurité intérieure qui permet désormais aux services habilités à cet effet de solliciter, pour les seules finalités et dans les conditions prévues par ce texte, des autorisations d'exploitation concernant des identifiants techniques rattachables au territoire national, d'où communique l'utilisateur.

2.2 Un examen attentif des motifs invoqués par les services dans leurs demandes d'autorisation de mise en œuvre de techniques de renseignement et un encadrement proportionné

2.2.1. La procédure de demande de renseignements complémentaires : un outil répondant au besoin d'information complète de la CNCTR

Dans son premier rapport d'activité, la CNCTR décrivait la procédure suivie lorsqu'elle reçoit une demande nécessitant une information plus complète de la commission[57]. Il peut s'agir d'une demande qu'elle estime insuffisamment motivée, difficile à apprécier ou d'une légalité incertaine. Mise en place lors de l'installation de la CNCTR pour favoriser le dialogue avec les services, cette procédure permet à la commission de demander au service concerné, ou à son ministre de tutelle, des renseignements complémentaires. Les précisions qu'elle demande portent, en règle générale, sur des questions de fond ou sur les modalités de mise en œuvre d'une technique, la commission ne s'estimant en mesure de pouvoir rendre un avis au Premier ministre que lorsqu'elle est en possession de tous les éléments permettant de comprendre une demande et d'apprécier la proportionnalité des mesures envisagées. Il revient ensuite au service concerné de lui communiquer, s'il en dispose, les éléments demandés, voire, si cela s'avère nécessaire, de compléter sa demande par des informations supplémentaires de nature à étayer la motivation qui la fonde. Selon les cas, le dialogue mené avec le service permettra à la commission de s'assurer que la personne ciblée est, de façon plausible, personnellement impliquée dans un projet susceptible d'affecter les intérêts fondamentaux de la Nation, que la menace qu'elle représente ou les intérêts publics invoqués à l'appui de sa demande peuvent justifier le recours à la mesure de surveillance sollicitée, voire, que les conditions envisagées de sa mise en œuvre sont conformes aux prescriptions légales,

57 - Voir le point 3.1 du premier rapport d'activité 2015-2016 de la CNCTR consacré aux fondements et aux principes de ses avis préalables.

notamment si l'opération de surveillance nécessite de pénétrer dans un lieu privé. Par ailleurs, lorsqu'une demande visant à renouveler la mise en œuvre d'une technique nécessite pour la CNCTR d'être mieux informée, le dialogue avec le service demandeur permettra à la commission d'obtenir les éléments de traçabilité des opérations réalisées lors de cette mise en œuvre ou toute précision utile s'y rapportant. Enfin, dans certaines circonstances particulières, la commission pourra vérifier auprès du service que les faits décrits dans sa demande sont bien distincts de ceux dont l'autorité judiciaire, le cas échéant, a été saisie. Dans tous les cas, les délais impartis par la loi à la commission pour rendre son avis courent à compter de la réception par celle-ci des éléments complétant la demande[58].

Le recours à cette procédure permet à la commission d'approfondir son contrôle *a priori*. Elle peut ainsi mieux discerner les demandes entachées d'une illégalité justifiant un avis défavorable de celles qui, bien que justifiées, sont maladroitement formulées ou insuffisamment précises.

Au cours de l'année 2019, la CNCTR a adressé 1 732 demandes de renseignements complémentaires aux services selon la répartition suivante :

- 836 demandes de renseignements complémentaires en matière d'accès aux données de connexion en temps différé[59] sur un total de 39 619, soit 2,1 % d'entre elles ;
- 896 demandes de renseignements complémentaires sur les autres demandes de techniques de renseignement[60], sur un total de 36 057 demandes, soit 2,5 % d'entre elles.

Ces éléments chiffrés témoignent d'une mise en œuvre ciblée de cette procédure, en légère progression par rapport à l'année précédente au cours de laquelle :

- 729 demandes de renseignements complémentaires avaient été adressées en matière d'accès aux données de connexion en temps différé sur un total de 46 184, soit 1,6 % d'entre elles ;

58 - En l'absence de réponse du service dans un délai de quinze jours, le GIC adresse à ce dernier une invitation à produire les éléments réclamés par la CNCTR dans un nouveau délai de quinze jours. Si cette invitation demeure également sans réponse, la demande est réputée abandonnée.

59 - Voir l'article L. 851-1 du code de la sécurité intérieure.

60 - Il s'agit des autres techniques prévues par le titre V du livre VIII du code de la sécurité intérieure.

- 521 demandes de renseignements complémentaires avaient été adressées sur les autres demandes de techniques de renseignement, sur un total de 28 085, soit 1,9 % d'entre elles.

Les développements informatiques réalisés par le GIC ont largement contribué à l'efficacité de cette procédure, en assurant une mise en œuvre dématérialisée fluide, rapide et sécurisée.

2.2.2 Les restrictions apportées par la CNCTR aux durées de validité des techniques de renseignement sollicitées : un ajustement précis des avis de la commission limitant au plus près les atteintes au droit au respect de la vie privée

Dans son premier rapport d'activité[61], la CNCTR indiquait que ses avis favorables pouvaient être assortis d'observations ou de restrictions relatives aux conditions de mise en œuvre d'une technique de renseignement.

Les restrictions dont sont assortis les avis de la commission peuvent porter sur la durée de validité de l'autorisation de mise en œuvre d'une technique de renseignement, la CNCTR recommandant alors une durée inférieure à la durée maximale prévue par la loi.

De telles restrictions peuvent s'appliquer lorsqu'un service n'est pas en mesure de renseigner l'identité de la personne visée dans sa demande. Si la commission estime que les enjeux invoqués par le service sont d'une gravité telle qu'ils peuvent justifier le recours à la technique sollicitée, y compris sur une personne non identifiée, elle préconisera alors de limiter la durée pendant laquelle peut être autorisée l'utilisation de cette mesure. Elle demandera au service concerné qu'au cours de cette période plus limitée de mise en œuvre de la technique, lui soient rapidement fournis les éléments d'identification manquant dans la demande initiale ainsi que tout renseignement recueilli permettant de confirmer que la personne visée est

61 - Voir le point 3.1 du premier rapport d'activité 2015/2016 de la CNCTR.

personnellement impliquée dans un projet susceptible d'affecter les intérêts fondamentaux de la Nation sur le fondement desquels sa surveillance a été autorisée.

La CNCTR peut aussi préconiser de limiter la période d'utilisation d'une technique à la durée d'un événement ponctuel, qui seul justifie la demande de surveillance.

Dans tous les cas, les techniques mises en œuvre dans ces conditions plus restrictives font l'objet d'un suivi particulièrement attentif de la part de la commission dans le cadre de son contrôle *a posteriori*.

Cette faculté que la loi confie à la CNCTR est conçue comme un outil à sa disposition pour exercer pleinement son contrôle de proportionnalité et limiter l'atteinte à la vie privée des personnes concernées. Son usage impose aux services de saisir la commission dans des délais plus courts que ceux que prévoit la loi pour demander l'autorisation de poursuivre une surveillance soumise à de telles restrictions. Il peut en résulter un nombre accru de demandes de renouvellement d'autorisation et, corrélativement, du nombre d'avis rendus par la CNCTR sur ces demandes. Ce facteur doit être pris en compte dans l'interprétation des statistiques de demandes de techniques de renseignement.

3. Le contrôle *a posteriori* de la mise en œuvre des techniques autorisées : la poursuite de l'approfondissement du contrôle

Comme elle l'indiquait dans ses précédents rapports d'activité[62], la CNCTR a recours, dans le cadre de sa mission de contrôle de la mise en œuvre des techniques de renseignement, à deux méthodes pour s'assurer de la conformité du recueil, de la transcription, de l'extraction[63] et de la conservation des renseignements aux dispositions du livre VIII du code de la sécurité intérieure.

D'application quotidienne, la première méthode consiste, pour la commission, à opérer des vérifications depuis ses locaux grâce aux outils informatiques mis à sa disposition par le GIC.

Ces applications lui offrent un accès direct aux données recueillies[64], voire, pour certaines techniques, aux transcriptions et extractions effectuées à partir de ces données.

La seconde méthode consiste en la réalisation de contrôles sur pièces et sur place au sein des services de renseignement, ces contrôles pouvant porter sur l'intégralité des techniques entrant dans le champ de compétence de la commission.

---

62 - Voir les points 4.1 et 4.2 du premier rapport d'activité 2015/2016 de la CNCTR, le point 2.2 de son deuxième rapport d'activité 2017 ainsi que le point 2.2 de son troisième rapport d'activité 2018.

63 - Voir le point 2.2.1 du troisième rapport d'activité 2018 de la CNCTR dans lequel elle rappelle que l'exploitation des données recueillies peut prendre la forme d'extractions, lorsqu'une partie de ces données, par exemple une image ou une parole, est prélevée, ou de transcriptions, lorsque des données brutes font l'objet d'une transformation destinée à en faciliter l'analyse.

64 - Les contrôles exercés par la CNCTR depuis ses locaux peuvent porter sur les accès aux données de connexion en temps différé (article L.851-1 du code de la sécurité intérieure), les géolocalisations en temps réel (article L. 851-4 du même code), le balisage (article L. 851-5 du même code), les interceptions de sécurité réalisées *via* le GIC (I de l'article L. 852-1 du même code).

Diligentés par une équipe composée de chargés de mission présentant des profils à la fois juridiques et techniques et, sauf impossibilité, d'un membre de la commission – le plus souvent la personnalité qualifiée –, ces contrôles sont menés à un rythme de deux, voire trois par semaine, tous services confondus.

Après avoir fortement progressé en 2017 jusqu'à atteindre plus de 120 en 2018, le nombre de contrôles sur pièces et sur place s'est stabilisé à plus d'une centaine en 2019, dont plus d'une vingtaine portant sur la surveillance internationale.

3.1 Le contrôle du recueil et de l'exploitation des données : entre avancées notables et améliorations attendues

La CNCTR dresse un bilan positif des contrôles sur pièces et sur place réalisés au cours de l'année 2019 et se montre, de manière générale, satisfaite des conditions d'accueil qui lui ont été réservées.

Dans la continuité de la démarche initiée dans son précédent rapport d'activité[65], elle constate que des progrès ont été réalisés mais que des améliorations sont encore attendues pour renforcer la précision et l'efficience du contrôle *a posteriori* dont elle est chargée par la loi.

3.1.1 La conformité aux exigences du cadre juridique : une situation globalement saine en dépit de quelques irrégularités

La CNCTR constate, à travers l'exercice de son contrôle *a posteriori*, que les services respectent les obligations légales qui leur incombent. Elle a cependant pu relever certaines irrégularités. La plupart d'entre elles ont été signalées aux services concernés au cours des contrôles et rapidement corrigées par ceux-ci. Dans deux cas, la CNCTR a choisi de saisir formellement le service par un courrier lui recommandant certaines mesures correctrices.

Les irrégularités les plus couramment observées et qui ont été corrigées sans formalisation d'une recommandation écrite par la commission se répartissent en trois catégories.

Afin de limiter les atteintes au droit au respect de la vie privée des personnes faisant l'objet de techniques de renseignement, **la loi a prévu que les**

65 - Voir le point 2.2.1 du troisième rapport d'activité 2018 de la CNCTR.

renseignements collectés doivent être détruits avant l'expiration d'un certain délai[66], dont la durée varie en fonction de la nature des données et de l'atteinte portée au droit au respect à la vie privée. Les opérations de destruction doivent être réalisées par des agents habilités et désignés à cet effet et faire l'objet de relevés auxquels la commission a accès.

La CNCTR a constaté dans huit cas un dépassement de la durée légale de conservation des données brutes recueillies dans la mise en œuvre de mesures de surveillance.

Par ailleurs, en application de l'article L. 822-3 du code de la sécurité intérieure, les transcriptions et les extractions peuvent être conservées tant qu'elles demeurent indispensables à la poursuite des finalités qui ont motivé leur réalisation. Dans un cas, la CNCTR a constaté que de telles transcriptions ou extractions étaient indûment conservées dans la mesure où leur lien avec la finalité poursuivie était contestable.

La deuxième catégorie d'irrégularités constatées a trait au dépassement de la durée d'autorisation de la mesure de surveillance. La CNCTR en a fait le constat à trois reprises. Dans tous les cas, le dépassement était de très courte durée. Dans deux cas, le service avait omis d'interrompre une technique au terme d'une première période de surveillance et alors que la demande de renouvellement de cette surveillance était en instance d'instruction.

La CNCTR estime qu'aucune de ces irrégularités n'a révélé une volonté délibérée de dissimulation ou de contournement des dispositions légales et qu'elles relèvent davantage de négligences ou d'insuffisances dans la gestion et le suivi de la mise en œuvre des techniques de renseignement.

Pour les deux catégories d'irrégularités ci-dessus décrites, la CNCTR a veillé à ce que les données irrégulièrement conservées ou les renseignements collectés en dehors des périodes d'autorisation soient détruits dans les plus brefs délais.

La CNCTR exige du service qu'il précise dans sa demande, pour certaines techniques complexes, les modalités qu'il entend mettre en

66 - Voir, notamment, les dispositions de l'article L. 822-2 du code de la sécurité intérieure.

œuvre afin de s'assurer du respect du cadre légal. Le service est en outre tenu de faire figurer dans des « fiches de traçabilité », c'est-à-dire des relevés de mise en œuvre, accessibles à la CNCTR depuis ses locaux, les modalités effectives de réalisation de chaque technique autorisée.

La plupart des services s'acquittent avec rigueur et diligence de leurs obligations en matière de traçabilité. Néanmoins, des retards ou, de façon plus rare, des carences de production des « fiches de traçabilité » sont parfois constatés. Lorsque c'est le cas, la commission sollicite le service et peut, lorsqu'elle s'estime insuffisamment informée sur les conditions de mise en œuvre d'une première autorisation, différer son avis sur une éventuelle demande de renouvellement dans l'attente des informations manquantes.

Des divergences entre les modalités de mise en œuvre d'une surveillance, indiquées par le service dans sa demande d'autorisation, et celles effectivement employées, ont été constatées dans un dossier. Le service a été invité à en expliquer les raisons qui se sont révélées être d'ordre opérationnel.

Les contrôles sur pièce et sur place ont dans un autre cas permis de déceler des écarts entre les mentions portées dans les fiches de traçabilité et la mise en œuvre effective de la technique. Ces discordances concernaient le matériel précisément utilisé pour exercer la surveillance. Le service a été prié de s'expliquer sur ce qui s'est révélé être une erreur matérielle et de rectifier la fiche de traçabilité.

Dans deux cas, la CNCTR a estimé nécessaire d'exercer de manière formelle son pouvoir de recommander, en application des dispositions de l'article L. 833-6 du code de la sécurité intérieure, que la mise en œuvre d'une technique soit immédiatement interrompue et que les renseignements collectés ainsi que les extractions et transcriptions effectuées soient détruits. Ces deux cas, relevant de deux services différents, concernaient la surveillance de personnes exerçant une profession ou un mandat protégés en application des dispositions de l'article L. 821-7 du code de la sécurité intérieure.

Dans les deux cas, la CNCTR s'est aperçue, à l'occasion de l'instruction de demandes de renouvellement de techniques de renseignement, que la cible exerçait une profession ou un mandat protégés. Les vérifications alors conduites par la CNCTR ont, en effet, permis d'établir que l'exercice de ces professions ou mandats, ignoré par le service lors de la première demande

d'autorisation de surveillance, avait par la suite été révélé par cette surveillance.

La CNCTR a immédiatement examiné chacun des deux cas en séance plénière, comme la loi l'exige lorsqu'est demandé le recours à une mesure de surveillance sur le territoire national concernant un parlementaire, un magistrat, un avocat ou un journaliste. Elle a estimé que la surveillance sollicitée ne pouvait être détachée de l'exercice du mandat ou de la profession et elle a, en conséquence, émis un avis défavorable au renouvellement des techniques sollicitées. Elle a, en outre, adressé aux chefs des services demandeurs, à leur ministre de tutelle ainsi qu'au Premier ministre, des recommandations d'interruption immédiate des surveillances en cours et de destruction de tous les renseignements recueillis ainsi que de toutes les transcriptions et extractions éventuellement réalisées.

La CNCTR a pu s'assurer que ces recommandations avaient été intégralement mises en œuvre sans qu'il fût besoin de faire usage de la faculté, offerte par les dispositions de l'article L. 833-8 du code de la sécurité intérieure, de saisir le Conseil d'État d'un recours.

3.1.2 La gestion des anomalies par la commission : un accompagnement renforcé des services dans leurs efforts de prévention et de régularisation rapide

Le constat d'une irrégularité, quelle que soit la suite que la CNCTR entend lui réserver, donne systématiquement lieu à un échange approfondi avec le service concerné. Il s'agit d'identifier précisément la ou les étapes des processus internes au cours desquels est survenue l'irrégularité afin de déterminer les éventuels ajustements à apporter pour prévenir toute réitération.

La commission estime en effet que, si l'article L. 833-6 du code de la sécurité intérieure lui accorde la faculté d'adresser une recommandation au service concerné tendant à l'interruption d'une technique de renseignement et à la destruction de renseignements indûment collectés, sa mission ne saurait se limiter à cette démarche. Elle cherche ainsi à accompagner et, dans certains cas, à guider la mise en œuvre de bonnes pratiques au sein des services de renseignement pour assurer le plein respect du cadre légal.

Depuis 2017, chaque service de renseignement est plus particulièrement suivi par deux ou trois référents attitrés parmi les agents du secrétariat général de la CNCTR. Le rôle de ces référents est de faciliter le dialogue quotidien avec les services afin de prévenir les irrégularités et, partant, de renforcer la sécurité juridique des activités de renseignement.

Dans le prolongement de cette démarche s'est également développée une pratique de consultation informelle de la commission sur les difficultés d'interprétation du cadre légal rencontrées par les services.

Ces échanges réguliers sont l'occasion, pour les services, d'exprimer leurs besoins opérationnels et, pour la CNCTR, de diffuser et d'expliquer sa doctrine. Ils contribuent à la prévention et à la réduction des irrégularités dans la mise en œuvre des techniques de renseignement.

3.1.3 La centralisation des données recueillies et la traçabilité de leur exploitation : un chantier qui progresse mais reste ouvert

3.1.3.1 De nouveaux outils et applications informatiques en cours d'appropriation par les services

Comme le rappelait la CNCTR dans son troisième rapport d'activité pour l'année 2018, l'action des services de renseignement est encadrée par les deux exigences légales complémentaires que sont la centralisation des renseignements collectés et la traçabilité des mesures d'exploitation de ces renseignements.

S'agissant de la centralisation, essentielle pour assurer un contrôle *a posteriori* efficace et pertinent, celle-ci a connu de notables progrès en 2019 mais demeure encore inachevée.

Après avoir défini, en 2017, les modalités de la centralisation des paroles et des images captées sur le fondement des dispositions de l'article L. 853-1 du code de la sécurité intérieure et expérimenté le dispositif au cours de l'année 2018 en matière de captation de paroles puis d'images, dans trois services

« pilotes », le GIC a généralisé celui-ci à tous les services de renseignement concernés[67] au cours de l'année 2019.

La majorité des techniques de renseignement sont ainsi couvertes par le dispositif de centralisation des renseignements collectés dans le système d'information du GIC, à l'exception des techniques de recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) et de celles de recueil et de captation de données informatiques (article L. 853-2 du même code), toutes deux caractérisées par une collecte décentralisée et des modalités diverses de stockage des données recueillies.

Le dispositif est, d'un point de vue technique, finalisé et opérationnel. Cependant, les retards pris dans la formation des personnels des services, les difficultés pratiques rencontrées lors du déploiement des matériels et des logiciels ainsi que les délais nécessaires à l'appropriation des nouvelles méthodes de travail qu'il nécessite ont retardé son utilisation effective.

Les projets de développement de réseaux informatiques sécurisés capables d'acheminer des données volumineuses ont, quant à eux, connu peu d'avancées au cours de l'année écoulée, laissant ainsi subsister un stockage décentralisé au sein d'échelons territoriaux de certains services. En conséquence, la CNCTR a mené, comme les années précédentes, plusieurs contrôles sur pièces et sur place dans des unités territoriales des services de renseignement.

S'agissant de la traçabilité de l'exploitation des données, la CNCTR constate que la tendance positive initiée en 2017 et confirmée en 2018, s'est maintenue en 2019.

D'une part, la CNCTR a, de manière générale, observé des progrès dans la rédaction des fiches de traçabilité, dès la fin de la mise en œuvre d'une technique ou, en l'absence de mise en œuvre, dès l'arrivée à échéance de l'autorisation. Ces fiches se révèlent souvent utiles à la préparation des

67 - Tous les services de renseignement sont tenus de recourir au dispositif géré par le GIC, hormis la DGSI et la DGSE, qui en ont la faculté mais non l'obligation. Ces deux services disposent, en effet, d'un dispositif propre de centralisation des renseignements recueillis.

contrôles *a posteriori*, en particulier pour affiner la sélection des dossiers que la CNCTR souhaite contrôler. La commission salue, à ce titre, la diligence avec laquelle la plupart des services s'efforcent de renseigner ces fiches de traçabilité, même si, comme elle l'a indiqué précédemment, quelques retards ou irrégularités ont pu être relevés[68].

D'autre part, la CNCTR constate que les développements informatiques assurant la traçabilité des consultations et de l'exploitation des renseignements collectés ont, cette année, comme l'année précédente, inégalement progressé.

Les services déjà dotés de ces dispositifs les ont en revanche corrigés et améliorés de sorte qu'ils se révèlent désormais particulièrement utiles et efficaces lors des contrôles *a posteriori* menés par la CNCTR.

3.1.3.2 La mise en œuvre des techniques de renseignement par les services : un cadre d'emploi rénové et des bonnes pratiques diffusées auprès des agents

La prise en compte progressive des exigences de centralisation et de traçabilité imposées par la loi du 24 juillet 2015 a conduit à des modifications importantes des procédures internes propres à chaque service.

Elle implique, en effet, des transformations significatives au sein de chaque service de renseignement, en particulier une homogénéisation des outils informatiques, tenus de garantir à la fois un niveau élevé de sécurité et un niveau de fonctionnalité au moins équivalent à celui des méthodes et des outils jusqu'alors utilisés.

De nouvelles consignes de mise en application du cadre légal ont, en outre, été élaborées en concertation avec la CNCTR et le GIC. Elles ont conduit à une formalisation plus importante du cadre d'emploi des dispositifs techniques utilisés. Plusieurs services ont notamment rédigé des guides méthodologiques pour chaque métier impliqué dans la mise en œuvre d'une technique de renseignement, de l'enquêteur ou de l'analyste sollicitant la surveillance à l'agent technique et opérationnel intervenant sur le terrain.

68 - Voir le paragraphe 3.1.1.3 du présent rapport.

En outre, au-delà de ces consignes internes propres à chaque service, le Premier ministre a diffusé aux quatre ministères concernés, à l'attention des agents des services, un document élaboré par le GIC après consultation de la CNCTR. Ce document à visée pratique décline les obligations légales en exemples concrets. Le GIC dispense également des formations aux agents des services.

3.1.4 Les fichiers de souveraineté : la persistance d'une limite à l'exercice par la commission de son pouvoir de contrôle des données recueillies par les services de renseignement

Tout en maintenant un rythme élevé de contrôles sur pièces et sur place, la commission a souhaité, en 2019, dans la continuité de l'orientation engagée l'année précédente, concentrer ses efforts de contrôle sur la phase d'exploitation des données recueillies, en particulier la réalisation, la diffusion et la conservation des transcriptions et extractions de ces données.

La CNCTR rappelle qu'elle dispose en effet, en application du 2° de l'article L. 833-2 du code de la sécurité intérieure, d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions. Cet accès est garanti par la loi, quels que soient les supports, fichiers ou documents comportant des éléments obtenus grâce à la mise en œuvre d'une technique de renseignement[69].

La volonté d'approfondissement du contrôle *a posteriori* manifestée par la commission s'est toutefois heurtée au refus, presque unanime, opposé par les services de renseignement de lui permettre d'accéder aux données contenues dans les fichiers intéressant la sûreté de l'État au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, communément dénommés « fichiers de souveraineté »[70]. Ces services justifient leur position par le fait que, outre les données issues de techniques de renseignement, figureraient dans ces fichiers des données de

69 - Voir le point 2.2.2 du deuxième rapport d'activité 2017 de la CNCTR ainsi que le point 2.2.1 de son troisième rapport d'activité 2018.

70 - Voir notamment l'article R. 841-2 du code de la sécurité intérieure.

provenances différentes, incluant des éléments communiqués par des services étrangers ou des éléments susceptibles de donner connaissance, directement ou indirectement, de l'identité des sources des services de renseignement, non soumis au contrôle de la CNCTR[71].

Des solutions alternatives à l'accès aux fichiers de souveraineté ont été proposées à la commission afin qu'elle puisse exercer son contrôle sur les données issues de techniques de renseignement susceptibles de venir alimenter les notes, bulletins de renseignement et fichiers de souveraineté. Elles permettront des progrès en matière de centralisation des données et contribueront à améliorer l'efficacité des contrôles. Il convient donc de saluer les efforts fournis par certains services pour développer de nouvelles solutions techniques destinées à permettre à la CNCTR d'accéder à l'ensemble des transcriptions et extractions réalisées à partir de données recueillies au moyen de techniques de renseignement.

Toutefois ces solutions alternatives, en cours de développement, ne répondent qu'imparfaitement à l'exigence d'exhaustivité du contrôle que doit assurer la CNCTR. Elles ne permettront pas, en effet, de s'assurer que sont effectivement absentes des fichiers de souveraineté des données dont le recueil et l'exploitation n'ont pas fait l'objet d'une autorisation légalement délivrée alors que le recueil, l'exploitation et la conservation de ces données relèvent du champ d'application du livre VIII du code de la sécurité intérieure.

La CNCTR estime donc souhaitable d'être autorisée à accéder directement aux fichiers de souveraineté des services pour y exercer son contrôle *a posteriori* de la mise en œuvre des techniques de renseignement.

71 - Voir le 4° de l'article L. 833-2 du code de la sécurité intérieure.

3.2 Le groupement interministériel de contrôle (GIC) : un partenaire essentiel de la CNCTR contribuant à l'efficacité de sa mission de contrôle

Créé en 1960 pour centraliser la mise en œuvre des seules interceptions de sécurité, le GIC s'est profondément transformé pour tenir compte des évolutions législatives et réglementaires en matière de renseignement, pour adapter son organisation aux besoins des services de renseignement et pour maîtriser les transformations que le secteur des communications électroniques a connues.

Érigé en service à compétence nationale rattaché au Premier ministre en application de la loi du 24 juillet 2015[72], il est désormais chargé des missions suivantes :

- enregistrer les demandes puis les autorisations de mise en œuvre des techniques de renseignement délivrées par le Premier ministre après avis de la CNCTR ;
- recueillir les données auprès des opérateurs de communications électroniques et des fournisseurs de services sur Internet grâce à un pouvoir de réquisition et en assurer la conservation ;
- centraliser l'exécution des interceptions de sécurité ainsi que les opérations de transcription et d'extraction des communications interceptées et contribuer à la centralisation des renseignements collectés lors de la mise en œuvre des techniques dites de proximité ;
- concourir à la traçabilité de l'exécution des techniques de recueil de renseignement ;

72 - Le dispositif législatif a été complété par le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement. Les dispositions de ce décret régissant le GIC ont été codifiées aux articles R. 823-1, R. 823-2 ainsi qu'aux articles R. 851-6 à R. 851-8 du code de la sécurité intérieure.

- assurer la défense du Premier ministre lorsque le Conseil d'État est saisi par une personne souhaitant vérifier, après avoir préalablement exercé son droit à réclamation devant la CNCTR, qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard.

Ainsi placé au cœur du dispositif de mise en œuvre des techniques de renseignement, le GIC est devenu le correspondant privilégié de la CNCTR dans l'exercice de ses missions de contrôle aussi bien *a priori* qu'*a posteriori*.

3.2.1 Une étroite coopération entre le GIC et la CNCTR

La CNCTR exerce son contrôle en contact permanent avec le GIC.

Des réunions de travail sont régulièrement organisées entre la direction du GIC et le secrétariat général de la CNCTR. Y sont débattues diverses questions relatives aux difficultés d'ordre juridique ou technique relevées aussi bien par la commission dans l'exercice de ses missions de contrôle que par les services dans la formalisation de leurs demandes puis dans la mise en œuvre des techniques de renseignement.

Deux « référents » sont, par ailleurs, désignés parmi les agents de la CNCTR pour entretenir le dialogue avec les équipes juridiques et techniques du GIC.

En outre, un groupe de travail rassemblant l'ensemble des utilisateurs des applications informatiques développées par le GIC (services de renseignement et CNCTR) est périodiquement réuni à l'initiative de ce dernier afin d'évoquer les perspectives d'amélioration, et s'agissant plus spécifiquement de la commission, les moyens de faciliter son contrôle.

Enfin, pour assurer sa mission de conservation des données recueillies et de centralisation de leur exploitation, le GIC a densifié ses emprises sur le territoire national et bénéficie aujourd'hui d'un maillage étendu. Des délégations du GIC et de la CNCTR respectivement composées, d'une part, du directeur ou de son adjoint et d'un ou deux responsables des cellules de soutien de la zone géographique concernée et, d'autre part, du président,

d'un membre du collège et d'un chargé de mission, effectuent des visites conjointes de ces centres territoriaux afin de rencontrer les chefs des services de renseignement déconcentrés[73].

Ces réunions sont l'occasion d'échanger sur les problématiques territoriales spécifiques auxquelles ces échelons sont confrontés, sur les difficultés d'ordre technique rencontrées ainsi que sur les interrogations juridiques suscitées par l'application du cadre légal. Un bilan des techniques mises en œuvre et des résultats obtenus est réalisé avec chaque service déconcentré, certains avis rendus par la commission sont évoqués et expliqués en même temps que les règles de droit sont rappelées.

3.2.2 Des modalités de contrôle complémentaires

Grâce aux développements informatiques entrepris par le GIC depuis 2016 et qu'il s'attache à faire constamment progresser, la CNCTR est en mesure de réaliser, à tout moment, depuis ses locaux, des vérifications portant sur les données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), les géolocalisations en temps réel (article L. 851-4 du même code), le balisage (article L. 851-5 du même code) et les interceptions de correspondances émises par la voie des communications électroniques auprès des opérateurs (I de l'article L. 852-1 de ce code).

En matière d'interceptions de sécurité, le GIC exerce un contrôle du recueil et de l'exploitation des données recueillies et un contrôle des transcriptions ou extractions qui vient compléter et renforcer la mission de contrôle *a posteriori* de la CNCTR.

En matière de recueil et d'exploitation, le GIC réalise un contrôle attentif et soutenu sur l'état des identifiants techniques placés en interception. Ce contrôle vise à s'assurer que l'utilisateur effectif de la ligne correspond bien à la cible du service. Il porte également sur l'état de la ligne ou de tout autre

73 - Voir le point 2.2 du troisième rapport d'activité 2018 de la CNCTR. Il peut s'agir des services déconcentrés de la sécurité intérieure, de la police judiciaire, du renseignement territorial, de la gendarmerie nationale ou des enquêtes douanières.

vecteur utilisé pour acheminer la communication. Lorsqu'une anomalie est détectée, des échanges ont lieu entre le GIC et le service exploitant en vue de sa rectification. Cette procédure peut conduire à la suppression de l'identifiant intercepté lorsque l'anomalie ne peut être rectifiée.

La CNCTR procède à un contrôle complémentaire, en particulier à l'occasion de l'instruction des demandes de renouvellement des interceptions de sécurité. L'une des applications informatiques mises à sa disposition par le GIC lui permet, en effet, d'accéder aux comptes rendus des contrôles que celui-ci a effectués.

Lorsque la CNCTR constate que la demande porte sur un identifiant technique signalé par le GIC comme relevant d'une anomalie et qu'aucune réponse satisfaisante n'a été apportée par le service exploitant, elle fait application de la procédure de demande de renseignements complémentaires décrite précédemment[74] afin d'obtenir des explications. À défaut de réponse satisfaisante, elle pourra notamment recommander au Premier ministre d'exclure de l'autorisation sollicitée l'identifiant litigieux, demander au service de reformuler sa demande, voire émettre un avis défavorable à la demande.

La CNCTR a, par ailleurs, développé un dispositif propre de contrôle consacré aux anomalies dites « judiciaires » à partir des informations fournies par les applications informatiques mises à sa disposition par le GIC.

La CNCTR veille, en effet, à ce que les services de renseignement portent une attention scrupuleuse aux éventuelles interférences entre police judiciaire et police administrative, en faisant toujours prévaloir la primauté de l'autorité judiciaire, consacrée par l'article 66 de la Constitution.

Lorsqu'un identifiant placé sous interception de sécurité sur le fondement de l'article L. 852-1 du code de la sécurité intérieure fait, ultérieurement, l'objet d'une interception judiciaire, l'opérateur de communications électroniques sollicité pour cette interception en avise le GIC qui supprime l'identifiant de la liste de ceux associés à l'autorisation de mise en œuvre de la technique de renseignement. L'information est diffusée par le GIC à travers

74- Voir le point 2.2.1 du présent rapport.

ses outils informatiques et ainsi portée à la connaissance de la CNCTR et des services. La CNCTR recherche alors si d'éventuelles autres techniques de renseignement sont en cours sur l'identifiant faisant l'objet d'une interception judiciaire ainsi que sur la cible elle-même. Une courte période de « veille active » s'ouvre au cours de laquelle la commission laisse au service l'opportunité d'interrompre spontanément les techniques portant sur la cible. Au terme de cette première phase, la commission vérifie que la ou les techniques ont été effectivement supprimées.

Lorsqu'une ou plusieurs techniques de renseignement perdurent, la commission prend l'attache du service et l'invite, soit à justifier que les faits couverts par la procédure judiciaire en cours sont distincts, donc détachables, de ceux justifiant la poursuite de la surveillance administrative de la cible[75] soit, à défaut, à mettre un terme à ces techniques dans les plus brefs délais. Le GIC est destinataire de l'ensemble de ces échanges. Lorsque le service indique ne pas être en mesure de déterminer la nature et/ou le périmètre de la saisine de l'autorité judiciaire, la CNCTR lui impose de supprimer l'ensemble des techniques de police administrative en cours sur la cible.

En matière de suivi des « productions » issues des interceptions de sécurité, le GIC contrôle systématiquement l'ensemble des transcriptions et extractions effectuées par les exploitants des services.

Les opérations de transcription et extraction sont exclusivement réalisées dans les locaux du GIC, à partir d'une application informatique dédiée. Toutes les productions sont ensuite soumises à la validation du GIC avant de pouvoir être transmises au service et aux agents intéressés, sous forme d'un document imprimé ou par voie dématérialisée sécurisée. Lorsque l'une de ces opérations soulève une difficulté, le GIC sollicite des explications auprès du service. Si la difficulté ne peut être surmontée, le service ne peut disposer de la transcription litigieuse.

75 - C'est par exemple le cas lorsque la procédure judiciaire concerne une implication dans un trafic de stupéfiants alors que la cible est suivie au titre de la prévention du terrorisme sur le fondement de la loi du 24 juillet 2015.

La CNCTR exerce également, depuis ses locaux un suivi ponctuel de ces productions, soit de manière spontanée, soit de manière programmée, certains avis conditionnant le renouvellement de l'autorisation à la réalisation de ce contrôle.

Une vigilance particulière est, de surcroît, portée tant par le GIC que par la CNCTR aux transcriptions et extractions se rapportant à des cibles exerçant l'une des professions ou mandats protégés par les dispositions de l'article L. 821-7 du code de la sécurité intérieure[76]. Le contrôle préalable du GIC est ici doublé d'un contrôle de la CNCTR qui s'assure que l'atteinte, le cas échéant portée aux garanties attachées à l'exercice de ces professions ou mandats, est nécessaire et proportionnée aux finalités légales poursuivies.

En outre, lorsque le service de renseignement, le GIC ou la CNCTR découvre ou suspecte, au stade de l'exploitation des données recueillies, que la cible exerce en réalité une profession ou un mandat protégés, l'exploitation de l'interception de sécurité est immédiatement suspendue jusqu'à ce que le service procède aux vérifications nécessaires. Si la suspicion ou l'information se confirme, le service est tenu de présenter, pour être, le cas échéant, autorisé à reprendre l'exploitation, une demande de modification de l'autorisation dont il dispose qui sera alors examinée par la CNCTR réunie en formation plénière. L'interception de sécurité ne pourra être poursuivie que si les faits justifiant la demande de surveillance peuvent être regardés comme détachables de l'exercice des fonctions ou mandats exercés par la cible, et si la mesure de surveillance est nécessaire et proportionnée à la finalité poursuivie. Dans le cas contraire, la technique sera interrompue et l'ensemble des renseignements collectés et des transcriptions et extractions réalisées sera détruit.

76 - Il est rappelé qu'au terme de ces dispositions : « *Les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats.* »

4. Les recours contre la mise en œuvre des techniques de renseignement : un usage mesuré des recours administratifs et des recours contentieux

4.1 Une stabilité globale du nombre de réclamations adressées à la CNCTR

La CNCTR rappelle qu'elle peut être saisie par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Cette procédure préalable de réclamation est prévue par les dispositions de l'article L. 833-4 du code de la sécurité intérieure, en ce qui concerne la surveillance nationale, et par celles de l'article L. 854-9 du même code, en ce qui concerne la surveillance des communications électroniques internationales.

Comme la CNCTR le précisait dans ses précédents rapports d'activité[77], le pouvoir de vérification que la loi lui a confié porte sur les seules techniques de renseignement prévues au livre VIII du code de la sécurité intérieure, à savoir des techniques mises en œuvre par des services de renseignement pour des finalités administratives. Cette compétence n'inclut donc ni les mesures de surveillance ordonnées par l'autorité judiciaire ni celles, au demeurant illégales, que pratiqueraient des personnes privées.

La CNCTR souligne, par ailleurs, une nouvelle fois[78] que, pour des motifs de sécurité nationale, et en application des dispositions du décret n° 2015-1405

77 - Voir le point 5.1.1 du premier rapport d'activité 2015/2016, le point 3.1 du deuxième rapport d'activité 2017 et le point 2.2.3.1 du troisième rapport d'activité 2018.

78 - Cette obligation était précisée au point 5.1.1 du premier rapport d'activité 2015/2016.

du 5 novembre 2015 relatif aux exceptions à l'application du droit des usagers de saisir l'administration par voie électronique, elle ne peut valablement être saisie que par lettre envoyée par voie postale.

La réclamation doit être présentée par la personne concernée, justifiant de son identité, et mentionner, le cas échéant, les éléments techniques à partir desquels l'intéressé souhaite que les vérifications soient conduites. Ces éléments techniques, notamment des numéros de téléphone ou des adresses de messagerie électronique, doivent être assortis de justificatifs, par exemple un contrat d'abonnement ou une facture. Les vérifications ne peuvent avoir lieu que lorsque l'ensemble de ces informations et justificatifs a été communiqué à la commission.

La CNCTR instruit les réclamations qui lui sont adressées de la même manière et en utilisant les mêmes outils que lorsqu'elle effectue un contrôle *a posteriori* depuis ses locaux de sa propre initiative.

Le nombre de réclamations reçues par la CNCTR, en 2019, est en hausse par rapport à 2018 et se rapproche des chiffres atteints en 2016 et 2017. Il semble que la baisse constatée l'an passé ait été occasionnelle, le nombre moyen de réclamations adressées à la CNCTR au titre des années 2016, 2017 et 2019 étant de 50.

	2016	2017	2018	2019
Nombre de réclamations reçues par la CNCTR	49	54	30	47

Deux des réclamations reçues en 2019 ont été présentées par la même personne, celle-ci ayant par ailleurs déjà saisi la CNCTR les années précédentes et souhaitant que des vérifications soient à nouveau conduites à son sujet.

Le délai de réponse aux réclamations contenant toutes les informations nécessaires à leur traitement a été inférieur à deux mois.

Aucune réclamation n'a conduit la CNCTR à envoyer de recommandation au chef du service concerné, au ministre dont il relève ou au Premier ministre pour que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits, conformément à l'article L. 833-6 du code de la sécurité intérieure. En conséquence, la CNCTR ne s'est pas non plus trouvée dans la situation de devoir saisir le Conseil d'État d'un recours contentieux sur le fondement de l'article L. 833-8 du code, cette voie de recours étant ouverte lorsque le Premier ministre ne donne pas suite aux recommandations de la commission.

Le dispositif propre aux « lanceurs d'alerte »

Pour garantir qu'il soit mis fin aux éventuelles violations manifestes du cadre juridique applicable aux techniques de renseignement, l'article L. 861-3 du code de la sécurité intérieure prévoit que les agents des services de renseignement ayant connaissance, dans l'exercice de leurs fonctions, d'une telle violation, peuvent porter ces faits à la connaissance de la seule CNCTR. Il appartient alors à la commission, au vu des éléments qui lui ont été transmis, de faire usage le cas échéant des pouvoirs de contrôle que lui attribue la loi.

En 2019, la CNCTR n'a pas été saisie sur le fondement de l'article L. 861-3 du code de la sécurité intérieure. Ces dispositions n'ont pas reçu d'application depuis l'entrée en vigueur du nouveau cadre légal en 2015.

4.2 Un léger recul du nombre de recours formés devant le Conseil d'État

La procédure contentieuse spéciale prévue aux articles L. 773-1 et suivants du code de justice administrative permet de demander à une formation spécialisée du Conseil d'État de vérifier qu'une technique de renseignement n'est ou n'a pas été irrégulièrement mise en œuvre à l'encontre d'une personne. Les membres et le rapporteur public de la formation spécialisée sont habilités ès qualités à connaître d'informations couvertes par le secret de la défense nationale.

S'agissant des techniques de renseignement relevant de la surveillance intérieure, la formation spécialisée du Conseil d'État peut être saisie, sur le fondement de l'article L. 841-1 du code de la sécurité intérieure, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR.

En matière de surveillance des communications électroniques internationales, seul le président ou trois membres au moins de la commission peuvent présenter une requête au Conseil d'État, sauf s'il s'agit de vérifier la légalité de l'exploitation des communications de personnes utilisant des identifiants rattachables au territoire national et communiquant depuis la France. Dans ce dernier cas, toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR peut saisir le Conseil d'État, sur le fondement de l'article L. 854-9 du code de la sécurité intérieure.

En 2016, 2017 et 2018, le Conseil d'État avait respectivement été saisi de neuf, six et neuf requêtes concernant la mise en œuvre de techniques de renseignement.

Six décisions avaient été rendues en 2016, trois en 2017 et dix en 2018.

En 2019, six requêtes ont été enregistrées. Le Conseil d'État a statué sur quatre de ces requêtes ainsi que sur trois requêtes introduites en 2018.

Au 31 décembre 2019, cinq affaires demeuraient en instance (trois introduites en 2018 et deux en 2019.)

Comme les années précédentes, la CNCTR a produit des observations sur tous les recours qui lui ont été communiqués par le Conseil d'État.

La CNCTR ne s'est pas trouvée dans la situation d'exercer elle-même un recours contentieux devant le Conseil d'État sur le fondement des articles L. 833-8 ou L. 854-9 du code de la sécurité intérieure. Cette voie de recours est ouverte au président de la commission ou à trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission. En 2019, le Premier ministre a suivi tous les avis *a priori* défavorables émis par la CNCTR et les contrôles *a posteriori* effectués par la commission n'ont pas révélé d'irrégularité justifiant l'envoi d'une recommandation au Premier ministre.

Le dialogue institutionnel avec le Parlement, l'information du public et les relations internationales : une année marquée par l'approfondissement du dialogue avec les homologues européens

Au sein de la chaîne opérationnelle conduisant au recueil et à l'exploitation du renseignement, la CNCTR se voit confier par la loi une mission de contrôle qui ne peut, en application du principe de séparation des pouvoirs et eu égard aux exigences du secret de la défense nationale, être accomplie que par un organisme distinct non seulement du Gouvernement mais également du Parlement et du public. La commission se conçoit dès lors comme un « tiers de confiance », auquel le législateur a attribué une compétence spécialisée qu'il ne peut assurer directement. En retour, elle rend compte tout au long de l'année de ses activités au Parlement et au public, dans le respect du secret de la défense nationale qui couvre ses travaux en application de l'article L. 832-5 du code de la sécurité intérieure.

Par ailleurs, la commission conduit une action internationale destinée à faire connaître le cadre légal français applicable aux activités de renseignement ainsi qu'à recueillir les bonnes pratiques mises en œuvre par les institutions nationales de contrôle des pays partenaires de la France. Elle a approfondi cette année le dialogue avec ses homologues européens.

Dans le cadre du dialogue institutionnel avec le Parlement, le président de la CNCTR a été auditionné en juin 2019 par la délégation parlementaire au renseignement.

En juillet 2019, il a été reçu par le président du Sénat afin de lui présenter le troisième rapport d'activité de la commission pour l'année 2018.

Le président de la CNCTR a été entendu, lors de l'examen au Sénat du projet de loi de finances pour l'année 2020, par le rapporteur de la commission des lois saisie pour avis sur l'évolution des moyens alloués à la commission.

Outre la publication de son rapport annuel d'activité, la CNCTR entend faire connaître aux professionnels du droit, aux universitaires et à des associations de défense des libertés le cadre juridique applicable aux activités de renseignement.

En février 2019, invité par l'académie du renseignement à intervenir lors d'un colloque ouvert au public et consacré au droit du renseignement, le président de la CNCTR a présenté le cadre juridique créé par la loi du 24 juillet 2015 relative au renseignement et a décrit le fonctionnement de la commission.

S'agissant des relations internationales, la CNCTR s'est déplacée à Strasbourg en février 2019 pour y rencontrer la commissaire aux droits de l'homme du Conseil de l'Europe ainsi que des représentants de cette institution.

Elle a accueilli à Paris en mars 2019 le président d'une commission de contrôle néerlandaise, le *Commissie van toezicht op de inlichtingen en veiligheidsdiensten*.

En mars 2019, un membre de la CNCTR a représenté la commission lors d'une conférence organisée à Oslo par l'organisme de contrôle norvégien, le *Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*.

La CNCTR a reçu la visite d'une délégation d'experts représentant le gouvernement australien, en avril 2019, ainsi qu'une délégation parlementaire autrichienne, en mai 2019, pour une présentation du cadre juridique français applicable au renseignement.

En mai 2019, une réunion bilatérale s'est tenue à Paris avec la commission de contrôle néerlandaise.

En juin 2019, la CNCTR s'est rendue à Berlin pour s'entretenir avec les membres d'un organisme de contrôle allemand, l'*Unabhängiges gremium*.

Elle a accueilli à Paris en septembre 2019 le commissaire chargé du contrôle des activités de renseignement au Royaume-Uni, l'*Investigatory Powers Commissioner*.

Un représentant de la CNCTR a participé à une conférence sur le contrôle du renseignement, organisée à Londres en octobre 2019 par le rapporteur spécial des Nations unies sur le droit à la vie privée.

Une délégation de la CNCTR s'est déplacée à Madrid en octobre 2019 pour rencontrer le magistrat espagnol chargé, au sein du Tribunal suprême, du contrôle des activités de renseignement.

En décembre 2019, la CNCTR a participé à La Haye à la conférence européenne des autorités nationales de contrôle. Cette rencontre multilatérale, la deuxième de cette nature depuis la conférence de Paris organisée à l'initiative de la commission et de son homologue belge[79], a permis aux institutions participant à ce forum d'approfondir leur connaissance mutuelle et de poursuivre leur dialogue sur des enjeux d'intérêt commun liés notamment à l'évolution de la jurisprudence de la Cour européenne des droits de l'homme.

79 - Voir, pour une présentation détaillée de cette initiative, l'encadré intitulé « La conférence européenne des autorités nationales de contrôle » à la page 93 du troisième rapport d'activité 2018 de la CNCTR.

Annexes

Annexe n° 1

Délibération de la CNCTR n° 1/2019 du 2 mai 2019

Saisie pour avis le 19 avril 2019 par le ministre de l'intérieur[80] d'un projet de décret relatif à la désignation de certains services de la direction centrale de la police judiciaire pouvant être autorisés à mettre en œuvre des techniques de renseignement, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

Le projet de décret est pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que les services dits du « second cercle », c'est-à-dire autres que les services spécialisés de renseignement, peuvent être autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code lorsqu'ils sont désignés à cet effet par décret en Conseil d'État pris après avis de la CNCTR. Le décret doit préciser les techniques ainsi que les finalités mentionnées à l'article L. 811-3 du code qui peuvent faire l'objet d'autorisations.

En l'espèce, le ministre de l'intérieur indique à la CNCTR que la sous-direction de la lutte contre la criminalité organisée et la délinquance financière, au sein de la direction centrale de la police judiciaire, a été divisée en deux nouvelles entités, la sous-direction de la lutte contre la criminalité financière et la sous-direction de la lutte contre la criminalité organisée.

80 - Voir le courrier n° 2016 du 8 avril 2019, adressé au président de la CNCTR par le directeur des libertés publiques et des affaires juridiques du ministère de l'intérieur et reçu le 19 avril suivant.

L'ancienne sous-direction unique ayant été autorisée à recourir à des techniques de renseignement[81], le projet de décret soumis à la CNCTR a pour objet de remplacer, dans les dispositions réglementaires du code de la sécurité intérieure relatives au renseignement, la mention de cette sous-direction par les références aux deux nouvelles sous-directions.

En premier lieu, la CNCTR reprend l'ensemble des recommandations de portée générale énoncées notamment dans ses délibérations n° 2/2015 du 12 novembre 2015 et n° 2/2018 du 17 mai 2018. Ces recommandations définissent les principes devant, selon la commission, régir la mise en œuvre des techniques de renseignement par des services dits du « second cercle ».

En deuxième lieu, la CNCTR rappelle que la sous-direction de la lutte contre la criminalité organisée et la délinquance financière pouvait être autorisée à mettre en œuvre les techniques de renseignement suivantes :

- accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- balisage (article L. 851-5 du code de la sécurité intérieure) ;
- recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (article L. 852-1 du code de la sécurité intérieure) ;
- interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ;
- captation de paroles prononcées à titre privé et captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;

81 - Voir, d'une part, le décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure. Voir, d'autre part, le décret n° 2018-543 du 29 juin 2018 relatif à la désignation de certains services autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure.

- introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou un dispositif de captation d'images.

La seule finalité que pouvait invoquer la sous-direction pour mettre en œuvre ces techniques était la prévention de la criminalité et de la délinquance organisées, prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure.

La liste des techniques autorisables ainsi que l'unique finalité invocable avaient été fixées par le pouvoir réglementaire conformément aux recommandations formulées par la CNCTR dans ses délibérations n° 2/2015 du 12 novembre 2015 et n° 2/2018 du 17 mai 2018.

En troisième lieu, la CNCTR constate que :

- les deux nouvelles sous-directions ont, comme l'entité dont elles sont issues, pour mission la lutte contre la criminalité et la délinquance organisées et peuvent avoir besoin de recueillir des renseignements à titre préventif, même si leur activité principale demeure répressive ;
- les techniques de renseignement auxquelles les deux nouvelles sous-directions pourraient être autorisées à recourir sont les mêmes que celles que pouvait mettre en œuvre l'entité dont elles sont issues.

En quatrième lieu, près de trois ans et demi après l'entrée en vigueur du décret permettant à la sous-direction de la lutte contre la criminalité organisée et la délinquance financière de mettre en œuvre des techniques de renseignement, aucun élément ne conduit la commission à modifier les recommandations qu'elle avait formulées sur les techniques utilisables et la finalité invocable par cette sous-direction.

Il n'y a dès lors pas lieu, selon la CNCTR, de restreindre l'accès des deux nouvelles sous-directions aux techniques de renseignement au-delà de ce qui était prévu pour l'entité dont elles sont issues.

En conséquence, la CNCTR émet un avis favorable au projet de décret qui lui est soumis.

Annexe n° 2

Délibération de la CNCTR n° 2/2019 du 4 juillet 2019

Saisie pour avis le 23 mai 2019 par la garde des sceaux, ministre de la justice[82], d'un projet de décret modifiant la partie réglementaire du code de la sécurité intérieure et relatif à la désignation des services relevant du ministère de la justice autorisés à recourir aux techniques de renseignement mentionnées au titre V du livre VIII du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

I. Remarques de portée générale

Le projet de décret est pris pour l'application de deux dispositions législatives.

La première de ces dispositions, de portée générale, est l'article L. 811-4 du code de la sécurité intérieure, qui régit l'accès des services dits du « second cercle » aux techniques de renseignement. Ces services peuvent être autorisés à recourir à des techniques lorsqu'ils sont désignés à cet effet par décret en Conseil d'État pris après avis de la CNCTR. Le décret doit préciser les techniques ainsi que les finalités mentionnées à l'article L. 811-3 du code qui peuvent faire l'objet d'autorisations.

La seconde disposition législative, de portée spéciale, est l'article L. 855-1 du code de la sécurité intérieure, qui concerne le seul renseignement pénitentiaire. Cet article prévoit qu'un décret en Conseil d'État pris après avis de la CNCTR désigne les services de l'administration pénitentiaire qui

82 - Un courrier de saisine, daté du 21 mai 2019, a été adressé au président de la CNCTR par le directeur du cabinet de la garde des sceaux et reçu le 23 mai 2019.

peuvent être autorisés à recourir à certaines techniques de renseignement limitativement énumérées par la loi, aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

Les services du ministère de la justice chargés du renseignement pénitentiaire peuvent mettre en œuvre des techniques dans ces deux cadres, pour des finalités distinctes. Deux décrets en Conseil d'État[83] ont désigné à cet effet, en 2017, le bureau central du renseignement pénitentiaire, les cellules interrégionales du renseignement pénitentiaire et les délégations locales au renseignement pénitentiaire.

Préalablement consultée, la CNCTR avait rendu deux avis, l'un dans sa délibération n° 3/2016 du 8 décembre 2016 concernant l'intégration du renseignement pénitentiaire dans le régime général applicable aux services du « second cercle », l'autre dans sa délibération n° 1/2017 du 16 mars 2017 concernant le recours à des techniques dans le cadre propre au renseignement pénitentiaire aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires.

Dans le projet de décret en Conseil d'État soumis à présent à la CNCTR, la garde des sceaux souhaite modifier les textes réglementaires issus des décrets de 2017 :

- pour tenir compte, dans les deux régimes évoqués ci-dessus, de la création du Service national du renseignement pénitentiaire, service à compétence nationale qui se substitue au bureau central du renseignement pénitentiaire et aux échelons territoriaux correspondants ;
- pour modifier, dans le régime général applicable aux services du « second cercle », les conditions dans lesquels le nouveau Service national du renseignement pénitentiaire pourrait avoir recours aux techniques, en ouvrant ce recours à de nouvelles finalités et en élargissant le public susceptible d'être visé par les techniques.

---

83 - Voir, d'une part, le décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure et, d'autre part, le décret n° 2017-749 du 3 mai 2017 relatif à la désignation des services relevant du ministère de la justice pris en application de l'article L. 855-1 du code de la sécurité intérieure.

À titre liminaire, la CNCTR reprend l'intégralité des remarques de portée générale formulées dans ses précédents avis concernant le renseignement pénitentiaire, que constituent ses délibérations n° 3/2016 du 8 décembre 2016 et n° 1/2017 du 16 mars 2017. Ces remarques définissent les principes devant, selon la commission, régir la mise en œuvre des techniques de renseignement par des services du « second cercle ».

En premier lieu, la CNCTR considère que la nature et le nombre de techniques auxquelles peuvent avoir accès les services du « second cercle » dépend de la part qu'occupe le renseignement au sein de leurs missions ainsi que de l'expertise technique requise pour mettre en œuvre les techniques de manière sûre. Cette conception des besoins des services du « second cercle » en matière de techniques de renseignement, outre qu'elle est justifiée par la protection de la vie privée, est corroborée par la pratique observée depuis l'entrée en vigueur en décembre 2015, du premier décret en Conseil d'État désignant ces services.

En deuxième lieu, la CNCTR estime que les termes de l'article L. 811-4 du code de la sécurité intérieure permettent au service du « second cercle » demandeur soit de mettre en œuvre lui-même la technique, s'il en a la capacité, soit de faire réaliser l'opération par un opérateur technique, qui ne pourra en revanche participer à l'exploitation des renseignements collectés.

En troisième lieu, la CNCTR indique que l'ouverture, au profit d'un service de renseignement, de la faculté de mettre en œuvre des techniques pour une finalité particulière n'exclut pas que d'autres services de renseignement concernés par cette finalité continuent à agir de façon coordonnée et complémentaire, en fonction de leurs missions, de leurs compétences et de leur expertise technique.

En quatrième lieu, la CNCTR rappelle que l'exercice effectif de la mission de contrôle confiée à la commission par la loi nécessite qu'elle puisse, outre le contrôle *a priori* sur les demandes tendant à mettre en œuvre une technique, mener à bien un contrôle *a posteriori* sur les données recueillies. Ceci impose une centralisation de ces données, auxquelles la CNCTR doit avoir un accès permanent, complet et direct, conformément à l'article L. 833-2 du code de la sécurité intérieure. Pour les services du « second cercle », cette centralisation doit, du point de vue de la commission, être réalisée de préférence par le groupement interministériel de contrôle (GIC), service du Premier ministre.

II. Observations détaillées

1. Sur la création du Service national du renseignement pénitentiaire

La création du Service national du renseignement pénitentiaire (SNRP) nécessite de substituer, dans la partie réglementaire du livre VIII du code de la sécurité intérieure, la mention du nouveau service à celle du bureau central du renseignement pénitentiaire et des échelons territoriaux correspondants. C'est notamment l'objet des articles 2 à 8 du projet de décret. Cette substitution concerne aussi bien le régime général applicable aux services du « second cercle », prévu à l'article L. 811-4 du code de la sécurité intérieure, que le cadre propre au renseignement pénitentiaire, prévu à l'article L. 855-1 du même code, aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires.

L'arrêté du 29 mai 2019 portant création et organisation d'un service à compétence national dénommé « Service national du renseignement pénitentiaire » prévoit, à son article 2, que le SNRP a pour mission « *de rechercher, collecter, exploiter, analyser et diffuser les informations et renseignements susceptibles de révéler des risques d'atteinte aux intérêts fondamentaux de la Nation, à la sécurité des établissements pénitentiaires, des établissements de santé destinés à recevoir des personnes détenues et des services pénitentiaires* ».

L'arrêté du 29 mai 2019 dispose en outre, à son article 4, que le SNRP comprend :

- un échelon central ;
- des cellules interrégionales, placées sous l'autorité de l'échelon central ;
- des délégations locales au sein des établissements pénitentiaires, placées sous l'autorité de la cellule interrégionale territorialement compétente.

La CNCTR note que le SNRP poursuit les mêmes missions que son prédécesseur et s'appuie sur une organisation territoriale comparable. En cohérence avec son avis formulé dans sa délibération n° 3/2016 du 8 décembre 2016, la commission constate que cette organisation permet d'assurer le contrôle interne et la coordination des demandes tendant à la mise en œuvre des techniques de renseignement.

La CNCTR n'émet donc pas d'objection de principe à la substitution du SNRP aux services qui l'ont précédé, dans la partie réglementaire du livre VIII du code de la sécurité intérieure.

2. Sur les techniques de renseignement auxquelles le Service national du renseignement pénitentiaire pourrait être autorisé à recourir

S'agissant des techniques de renseignement auquel le SNRP pourrait avoir recours, le projet de décret ne modifie pas l'état du droit applicable jusqu'à présent au bureau central du renseignement pénitentiaire et aux échelons territoriaux correspondants.

a) En tant que service du « second cercle » relevant de l'article L. 811-4 du code de la sécurité intérieure, le SNRP aurait, en application du projet de décret, la faculté de mettre en œuvre :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) ;

- l'interception de correspondances par *IMSI catcher* (II de l'article L. 852-1 du code de la sécurité intérieure) ;
- l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- le recueil et la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé, y compris à usage d'habitation, pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images ou un dispositif de recueil ou de captation de données informatiques (article L. 853-3 du code de la sécurité intérieure).

La CNCTR rappelle que, dans ses délibérations n° 3/2016 du 8 décembre 2016 et n° 2/2018 du 17 mai 2018, elle avait émis un avis favorable à ce que les services du ministère de la justice chargés du renseignement pénitentiaire puissent être autorisés à mettre en œuvre l'ensemble des techniques ci-dessus, à l'exception de l'interception de correspondances par *IMSI catcher* prévue au II de l'article L. 852-1 du code de la sécurité intérieure.

La CNCTR avait en effet relevé que le II de l'article L. 852-1 du code de la sécurité intérieure encadrait de manière particulièrement restrictive l'utilisation d'*IMSI catchers* pour intercepter des correspondances. Elle avait estimé que le recours à cette technique devait être réservé à des services se consacrant exclusivement au renseignement, ce qui est le cas des services du ministère de la justice chargés du renseignement pénitentiaire. Toutefois, elle avait également considéré que la mise en œuvre de la technique nécessitait un niveau d'expérience et de technicité très élevé. À cet égard, la création récente des services concernés et leurs moyens tant humains que matériels encore modestes ne permettaient pas de regarder comme adapté leur accès à cette technique. En conséquence, la CNCTR avait émis un avis défavorable, en l'état, à la possibilité pour ces services d'intercepter des correspondances par *IMSI catchers*.

Au reste, le recours à cette technique n'étant justifié que dans des circonstances caractérisées par une urgence et une gravité telles que l'implication d'un service de renseignement du « premier cercle » serait nécessaire, la possibilité existait, en tout état de cause, *via* ces services de mettre en œuvre la technique en milieu pénitentiaire.

Constatant que cette analyse n'a pas été démentie par les deux premières années d'utilisation des techniques par les services du ministère de la justice chargés du renseignement pénitentiaire, la CNCTR en réaffirme la pertinence à l'égard du SNRP et émet un avis défavorable à ce que le nouveau service puisse être autorisé à mettre en œuvre des interceptions de correspondances par *IMSI catchers*. La commission recommande, en conséquence, de modifier l'article 4 du projet de décret pour prévoir la suppression de la mention du 4° de l'article R. 852-2 du code de la sécurité intérieure.

b) Au titre de la prévention des évasions et du maintien de la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues, finalité prévue à l'article L. 855-1 du code de la sécurité intérieure[84], le SNRP pourrait être autorisé à mettre en œuvre les techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) ;
- l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ;

84 - La rédaction en vigueur de cet article est issue de l'article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé, y compris à usage d'habitation, pour y mettre en place, utiliser ou retirer un dispositif de captation de paroles ou d'images (article L. 853-3 du code de la sécurité intérieure).

La liste de ces techniques est fixée par la loi. La CNCTR observe, en appui de son argumentation développée au point précédent, que, dans le cadre de l'article L. 855-1 du code de la sécurité intérieure, le législateur n'a pas ouvert aux services du ministère de la justice chargés du renseignement pénitentiaire la faculté de mettre en œuvre des interceptions de correspondances par *IMSI catchers*.

3. Sur les finalités pouvant justifier le recours aux techniques par le Service national du renseignement pénitentiaire

L'article L. 855-1 du code de la sécurité intérieure énonce la finalité pour laquelle les services du ministère de la justice chargés du renseignement pénitentiaire peuvent être autorisés à recourir aux techniques qu'il mentionne. Il s'agit de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

L'article L. 811-4 du code de la sécurité intérieure renvoie, quant à lui, à un décret en Conseil d'État la détermination des finalités, parmi celles mentionnées à l'article L. 811-3 du même code, que le SNRP pourrait invoquer dans ses demandes présentées en tant que service du « second cercle ». Jusqu'à présent, les services du ministère de la justice chargés du renseignement pénitentiaire pouvaient mettre en œuvre des techniques afin de prévenir le terrorisme, en application du 4° de l'article L. 811-3 du code, ou la criminalité et la délinquance organisées, en application du 6° de l'article L. 811-3 du code.

Le projet de décret reprend tout d'abord cet état du droit, que la CNCTR avait estimé adapté aux missions et aux besoins de l'administration pénitentiaire dans sa délibération n° 3/2016 du 8 décembre 2016.

La garde des sceaux envisage, en outre, deux évolutions.

a) Le projet de décret soumis à la CNCTR prévoit de rendre invocable par le SNRP la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure, à savoir la prévention :
   - des atteintes à la forme républicaine des institutions ;
   - des actions tendant au maintien ou à la reconstitution de groupements dissous ;
   - des violences collectives de nature à porter gravement atteinte à la paix publique.

La CNCTR rappelle, à titre liminaire, qu'elle se montre particulièrement vigilante sur l'invocation de la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure, considérant que la prévention de violences collectives ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, même extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.

En l'espèce, la CNCTR constate que, si les éléments dont elle dispose attestent un risque plausible que des personnes détenues organisent, favorisent ou coordonnent des actions violentes d'une gravité particulière depuis leur lieu de détention, le besoin de l'administration pénitentiaire porte sur la surveillance des communications électroniques de personnes détenues *via* internet. Un tel besoin peut, selon la commission, être satisfait par le recours à des accès administratifs à des données de connexion en temps différé, à des interceptions de sécurité ainsi qu'à des recueils de données informatiques, sans nécessiter la mise en œuvre d'autres techniques parmi les plus complexes et les plus intrusives, notamment celles soumises par la loi au respect du principe de subsidiarité. Les échanges informels entre la CNCTR et l'administration pénitentiaire au cours de l'instruction du projet de décret ont confirmé cette analyse.

Aussi la CNCTR émet-elle un avis favorable à ce que le SNRP puisse invoquer la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure à l'appui de demandes tendant à mettre en œuvre les techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) ;
- le recueil et la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure).

Elle émet, en revanche, un avis défavorable à ce que le SNRP puisse être autorisé à recourir, sur le fondement de la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure, aux autres techniques demandées, dont l'utilisation ne paraît pas justifiée au regard du besoin de l'administration pénitentiaire tel qu'il a été exposé à la CNCTR[85].

La CNCTR recommande, dès lors, que la référence à la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure soit limitée, dans les articles 3 et 5 du projet de décret, aux quatre techniques ayant fait l'objet d'un avis favorable de la commission et que cette même référence soit supprimée des articles 4, 6 et 7 du projet de décret.

85 - Les autres techniques demandées sont la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure), le balisage (article L. 851-5 du code de la sécurité intérieure), l'interception de correspondances par *IMSI catcher* (II de l'article L. 852-1 du code de la sécurité intérieure), l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure), la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) et l'introduction dans un lieu privé, y compris à usage d'habitation, pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images ou un dispositif de recueil ou de captation de données informatiques (article L. 853-3 du code de la sécurité intérieure).

b) Le projet de décret prévoit également que le SNRP puisse être désormais autorisé à s'introduire dans des lieux d'habitation pour mettre en place, utiliser ou retirer des dispositifs de surveillance sur le fondement de la finalité prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure, c'est-à-dire la prévention de la criminalité et de la délinquance organisées.

Les lieux d'habitation dans lesquels le service pourrait être autorisé à s'introduire sont, en l'espèce, les cellules de détention et les lieux assimilés, tels que les unités de vie familiale.

Dans sa délibération n° 3/2016 du 8 décembre 2016, la CNCTR avait considéré que la cellule de détention, bien que faisant partie des lieux mis à disposition et placés sous le contrôle de l'administration pénitentiaire, devait bénéficier d'un statut particulier. Si le personnel de l'administration pénitentiaire peut pénétrer dans la cellule, la fouiller ou effectuer des contrôles à l'œilleton, il s'agit en effet d'un lieu dans lequel la personne détenue se voit reconnaître une protection particulière de son intimité, tant en vertu des dispositions du code de procédure pénale que de la jurisprudence nationale et européenne.

La CNCTR en avait conclu que la cellule de détention et les lieux assimilés tels que les unités de vie familiale, en ce qu'ils abritent une part essentielle de la vie privée des personnes détenues, devaient être soumis au régime le plus protecteur prévu par la loi et, partant, être regardés, pour l'application du livre VIII du code de la sécurité intérieure, comme des lieux d'habitation au sens de l'article L. 853-3 de ce code. Des techniques ne pouvaient, dès lors, être mises en œuvre dans ces lieux sans que, outre l'autorisation d'y recourir, une autorisation d'introduction dans un lieu d'habitation ait été également accordée, après examen de la demande par la CNCTR réunie en formation collégiale.

Eu égard à ce contexte particulier, la CNCTR n'estime pas disproportionné l'octroi au SNRP de la faculté de s'introduire dans des lieux d'habitation pour mettre en place, utiliser ou retirer des dispositifs de surveillance sur le fondement de la finalité prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure, sous réserve que les lieux d'habitation concernés soient uniquement des cellules de détention ou des lieux assimilés, tels que des unités de vie familiale.

Au surplus, la CNCTR note que le législateur a récemment[86] permis que les services du ministère de la justice chargés du renseignement pénitentiaire, lorsqu'ils agissent dans le cadre prévu à l'article L. 855-1 du code de la sécurité intérieure, s'introduisent dans des lieux à usage d'habitation, sous réserve que les techniques mises en œuvre dans ces lieux ne visent que des personnes détenues. Cette disposition équivaut à limiter également, dans ce régime propre au renseignement pénitentiaire, la pénétration dans des lieux d'habitation aux cellules de détention et aux lieux assimilés.

En conséquence, la CNCTR émet un avis favorable, dans les conditions et limites énoncées ci-dessus, aux articles 6 et 7 du projet de décret, sous réserve que la rédaction de ces articles soit amendée pour garantir que les lieux d'habitation concernés soient uniquement des cellules de détention ou des lieux assimilés.

Les articles 6 et 7 du projet pourraient alors s'écrire comme suit :

« *Article 6.* - Le 4° du D du II de l'article R. 853-3 est ainsi rédigé : « 4° Service placé sous l'autorité du directeur de l'administration pénitentiaire : le Service national du renseignement pénitentiaire, pour mettre en œuvre à l'encontre des seules personnes détenues les dispositifs techniques mentionnés au premier alinéa du présent D, au titre des finalités prévues au 4° de l'article L. 811-3 et, par dérogation au même premier alinéa du présent D, au 6° de l'article L. 811-3. » ;

« *Article 7.* - Le 4° du F du II de l'article R. 853-3 est ainsi rédigé : « 4° Service placé sous l'autorité du directeur de l'administration pénitentiaire : le Service national du renseignement pénitentiaire, pour mettre en œuvre à l'encontre des seules personnes détenues les dispositifs techniques mentionnés au premier alinéa du présent F, au titre des finalités prévues au 4° de l'article L. 811-3 et, par dérogation au même premier alinéa du présent D, au 6° de l'article L. 811-3. ».

86 - Voir l'article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

4. Sur les personnes pouvant faire l'objet de techniques de renseignement mises en œuvre par le Service national du renseignement pénitentiaire

La CNCTR note que l'article L. 855-1 du code de sécurité intérieure, qui prévoit un régime de surveillance propre au renseignement pénitentiaire, autorise désormais[87] les services compétents du ministère de la justice à mettre en œuvre certaines techniques de renseignement à l'encontre de personnes autre que détenues, mais exclut que de telles personnes puissent faire l'objet de techniques nécessitant une introduction dans un lieu d'habitation.

S'agissant des compétences du SNRP en tant que service du « second cercle » régi par l'article L. 811-4 du code de la sécurité intérieure, le projet de décret prévoit, à son article 2, de supprimer la restriction prévue au III de l'article R. 811-2 du code de la sécurité intérieure, en vertu de laquelle les services du ministère de la justice chargés du renseignement pénitentiaire peuvent, en tant que services du « second cercle » régis par l'article L. 811-4 du même code, mettre en œuvre des techniques « *pour le seul exercice des missions qui sont assignées à l'administration pénitentiaire envers les personnes qui lui sont confiées par l'autorité judiciaire en application de l'article 2 de la loi du 24 novembre 2009* ».

La CNCTR avait recommandé, dans sa délibération n° 3/2016 du 8 décembre 2016, que les services du ministère de la justice chargés du renseignement pénitentiaire concentrent leur action sur les seules personnes détenues, qu'elles vivent intégralement en établissement pénitentiaire ou y soient seulement hébergées.

Eu égard aux arguments développés par la garde des sceaux, la commission estime justifiés les nouveaux besoins exprimés dans la saisine et n'émet pas d'objection à ce que le SNRP puisse mettre en œuvre des techniques de renseignement à l'encontre de personnes autres que détenues, sous réserve cependant que cette mise en œuvre ne nécessite pas d'introduction dans un

87 - Voir l'article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

lieu d'habitation qui ne serait pas une cellule de détention ou des lieux assimilés, tels que des unités de vie familiale. De telles intrusions relèveraient le cas échéant de l'activité d'autres services de renseignement.

Aussi la CNCTR émet-elle un avis favorable à la redéfinition, à l'article 2 du projet de décret, du public susceptible d'être surveillé par le SNRP, sous réserve que les articles 6 et 7 du projet, qui prévoient les cas dans lesquels le service pourrait s'introduire dans un lieu d'habitation, excluent de leur champ d'application les personnes autres que détenues. La commission a proposé, au point 3 du II de la présente délibération, une rédaction des articles 6 et 7 du projet garantissant le respect de cette réserve.

Dans les limites et sous les réserves formulées par la présente délibération, la CNCTR émet un avis favorable au projet de décret que lui a soumis la garde des sceaux.

Annexe n° 3

Délibération de la CNCTR n° 3/2019 du 10 juillet 2019

Saisie le 5 juillet 2019 pour avis par le Premier ministre d'un projet de décision fixant les trois contingents prévus à l'article L. 855-1 du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

L'article L. 855-1 du code de la sécurité intérieure prévoit que les services du ministère de la justice chargés du renseignement pénitentiaire peuvent être autorisés, aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires, à recourir à des techniques dont la liste a été récemment complétée par la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice[88].

Ont été ajoutées par cette loi :

- l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé ou la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé pour y mettre en place, utiliser ou retirer des dispositifs de captation d'images ou de paroles (article L. 853-3 du code de la sécurité intérieure).

88 - Voir la modification de l'article L. 855-1 du code de la sécurité intérieure résultant de l'article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

La loi soumet la mise en œuvre de ces techniques au respect d'un contingent, selon lequel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum arrêté par le Premier ministre après avis de la CNCTR.

Le Premier ministre se propose de fixer, pour chacun des trois articles mentionnés ci-dessus, un contingent d'autorisations accordées sur leur fondement égal à vingt.

Eu égard aux informations dont elle dispose sur les besoins opérationnels et les capacités techniques des services chargés du renseignement pénitentiaire, la CNCTR considère les contingents envisagés comme proportionnés.

En conséquence, la CNCTR émet un avis favorable à ce que les trois contingents prévus à l'article L. 855-1 du code de la sécurité intérieure s'élèvent à vingt autorisations maximales simultanément en vigueur.

Annexe n° 4

Délibération de la CNCTR n° 4/2019 du 7 novembre 2019

Saisie le 18 octobre 2019 pour avis par le Premier ministre, en application du I bis de l'article L. 851-2 du code de la sécurité intérieure, d'un projet d'augmenter le nombre maximal des autorisations de recueil de données de connexion en temps réel pouvant être accordées simultanément, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

La CNCTR rappelle que le contingent des autorisations simultanées de recueil de données de connexion en temps réel avait été fixé à 500, après avis favorable de la commission[89], par une décision du Premier ministre du 8 janvier 2018.

Le Premier ministre se propose de l'élever à 720.

La CNCTR a constaté que la technique du recueil de données de connexion en temps réel, qui ne peut être mise en œuvre que pour prévenir le terrorisme, présentait un intérêt opérationnel croissant pour les services de renseignement et que le contingent en vigueur était presque entièrement utilisé. Eu égard à la persistance d'une menace terroriste élevée, la commission estime avéré le besoin d'accorder simultanément un nombre supérieur d'autorisations. Elle considère que le chiffre de 720 ne porte pas à la vie privée une atteinte disproportionnée à la menace qu'il s'agit de prévenir.

En conséquence, la CNCTR émet un avis favorable à l'augmentation du contingent envisagée.

89 - Voir la délibération de la CNCTR n° 6/2017/CD du 7 décembre 2017.

Annexe n° 5

Délibération de la CNCTR n° 5/2019 du 7 novembre 2019

Saisie pour avis le 30 octobre 2019 par le ministre de l'intérieur[90] d'un projet de décret relatif à la désignation de certains services de la direction générale de la police nationale pouvant être autorisés à mettre en œuvre des techniques de renseignement, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

Le projet de décret est pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que les services dits du « second cercle », c'est-à-dire autres que les services spécialisés de renseignement, peuvent être autorisés à recourir aux techniques mentionnées au titre V du livre VIII du même code lorsqu'ils sont désignés à cet effet par décret en Conseil d'État pris après avis de la CNCTR. Le décret doit préciser les techniques ainsi que les finalités mentionnées à l'article L. 811-3 du code qui peuvent faire l'objet d'autorisations.

En l'espèce, le ministre de l'intérieur indique à la CNCTR que le projet de décret a pour but de tirer les conséquences de trois réformes structurelles devant entrer en vigueur le 1er janvier 2020 au sein de la direction générale de la police nationale :

- le rattachement de l'unité de coordination de la lutte antiterroriste (UCLAT) à la direction générale de la sécurité intérieure (DGSI) ;
- la création de l'office antistupéfiants (OFAST) ;
- la création de directions territoriales de la police nationale à Mayotte, en Guyane et en Nouvelle-Calédonie.

90 - Voir le courrier n° 2051 du 25 octobre 2019, adressé au président de la CNCTR par le directeur des libertés publiques et des affaires juridiques du ministère de l'intérieur et reçu le 30 octobre suivant.

À titre liminaire, la CNCTR reprend l'ensemble des recommandations de portée générale énoncées notamment dans ses délibérations n° 2/2015 du 12 novembre 2015 et n° 2/2018 du 17 mai 2018. Ces recommandations exposent les principes devant, selon la commission, régir la mise en œuvre des techniques de renseignement par les services dits du « second cercle ».

a) L'UCLAT, actuellement désignée comme un service du « second cercle »[91], est chargée d'une mission de coordination, d'animation et d'orientation des services de la police nationale en matière de lutte contre le terrorisme. N'ayant pas de rôle opérationnel, elle peut uniquement mettre en œuvre des recueils de données de connexion en temps différé prévus à l'article L. 851-1 du code de la sécurité intérieure, au titre de la prévention du terrorisme, des atteintes à la forme républicaine des institutions ou des actions tendant au maintien ou à la reconstitution de groupements dissous[92].

Le ministre de l'intérieur indique avoir décidé le rattachement de l'UCLAT à la DGSI pour confirmer le rôle prééminent confié à celle-ci en matière de lutte contre le terrorisme.

La CNCTR prend acte de ce rattachement, qui a pour conséquence d'intégrer l'UCLAT dans un service spécialisé de renseignement, dit du « premier cercle », pouvant être autorisé, en application du livre VIII du code de la sécurité intérieure, à mettre en œuvre toutes les techniques de renseignement au titre de toutes les finalités prévues par la loi.

Le projet de décret supprime dès lors, au 1° de ses articles 2 et 3, la référence à l'UCLAT des dispositions réglementaires régissant l'accès des services du « second cercle » aux techniques de renseignement. La CNCTR n'a pas de remarque à formuler sur ce point.

b) L'OFAST doit succéder à l'Office central pour la répression du trafic illicite des stupéfiants (OCRTIS). Actuellement compris dans la sous-direction de la lutte contre la criminalité organisée au sein de la direction centrale de

91 - Voir notamment l'article R. 811-2 du code de la sécurité intérieure, dans sa rédaction résultant du décret n° 2015 1639 du 11 décembre 2015.

92 - Ces finalités sont celles prévues au 4° et aux a) et b) du 5° de l'article L. 811-3 du code de la sécurité intérieure.

la police judiciaire, l'OCRTIS peut être autorisé à recourir à toutes les techniques de renseignement ouvertes à cette sous direction, qui a été désignée comme service du « second cercle »[93] ayant la faculté de mettre en œuvre des techniques au seul titre de la prévention de la criminalité et de la délinquance organisées[94].

Le ministre de l'intérieur indique que l'OFAST, service à compétence nationale, sera placé directement sous l'autorité du directeur central de la police judiciaire. Chargé tout d'abord d'évaluer la menace, le nouvel office aura également un rôle opérationnel lors d'enquêtes qu'il conduira seul ou en coordination avec les services territoriaux de la police ou de la gendarmerie nationales. Si la majeure partie de cette activité relève du régime applicable aux enquêtes judiciaires, l'OFAST pourra, comme son prédécesseur l'OCRTIS, avoir besoin de recueillir des renseignements à titre préventif.

Le projet de décret prévoit dès lors, au 2° de ses articles 2 et 3 et à son article 4, que l'OFAST soit désormais désigné en tant que tel comme service du « second cercle » et puisse être autorisé à mettre en œuvre, au seul titre de la prévention de la criminalité et de la délinquance organisées, les techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (article L. 852-1 du code de la sécurité intérieure) ;

93 - Voir notamment l'article R. 811-2 du code de la sécurité intérieure dans sa rédaction résultant du décret n° 2015 1639 du 11 décembre 2015.

94 - Cette finalité est celle prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure.

- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou un dispositif de captation d'images.

La CNCTR constate que ces techniques et la finalité invocable pour les mettre en œuvre sont les mêmes, à une exception près, que celles ouvertes à la sous-direction de la lutte contre la criminalité organisée. Sauf l'interception de sécurité effectuée sur des réseaux exclusivement hertziens, prévue à l'article L. 852-2 du code de la sécurité intérieure, l'OFAST pourra bénéficier pour ses enquêtes des mêmes techniques de renseignement que son prédécesseur l'OCRTIS.

La CNCTR rappelle que la liste des techniques autorisables ainsi que l'unique finalité invocable par la sous-direction chargée de la lutte contre la criminalité organisée et, partant, par l'OCRTIS avaient été fixées par le pouvoir réglementaire[95] conformément aux recommandations formulées par la CNCTR dans ses délibérations n° 2/2015 du 12 novembre 2015 et n° 2/2018 du 17 mai 2018.

Près de quatre ans après l'entrée en vigueur du décret permettant à l'OCRTIS de mettre en œuvre des techniques de renseignement, aucun élément ne conduit la commission à modifier les recommandations qu'elle avait formulées à cet égard. La CNCTR n'émet donc pas d'objection à ce que l'OFAST puisse être doté des compétences prévues par le projet de décret.

c) Les services déconcentrés de la police nationale à Mayotte, en Guyane et en Nouvelle Calédonie relèvent de différents services centraux, tels que la direction centrale de la sécurité publique ou la direction centrale de la police judiciaire. Comme leurs équivalents en métropole, ces services

95 - Voir les dispositions réglementaires du livre VIII du code de la sécurité intérieure, dans leur rédaction résultant du décret n° 2015-1639 du 11 décembre 2015, du décret n° 2018-543 du 29 juin 2018 et du décret n° 2019-684 du 28 juin 2019.

déconcentrés peuvent être autorisés à mettre en œuvre des techniques de renseignement pour certaines finalités prévues par la loi, en application du livre VIII du code de la sécurité intérieure[96].

Le ministre de l'intérieur indique à la CNCTR avoir décidé que les services déconcentrés de la police nationale seraient placés, dans chacun des trois territoires mentionnés ci-dessus, sous l'autorité d'une direction territoriale de la police nationale, afin d'améliorer l'efficacité de la gouvernance territoriale et de rendre plus visible l'action unifiée de la police nationale dans des territoires confrontés à une forte délinquance et à des mouvements contre l'ordre public.

Le projet de décret, à ses articles 5 à 9, désigne les nouvelles directions territoriales de la police nationale comme des services du « second cercle » et prévoit que certains services déconcentrés placés sous leur autorité, en l'espèce les services du renseignement territorial et les antennes de police judiciaire, pourront être autorisés à mettre en œuvre les techniques suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (article L. 852-1 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure), pour les seuls services du renseignement territorial ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise.

96 - Voir les dispositions réglementaires du livre VIII du code de la sécurité intérieure, dans leur rédaction résultant du décret n° 2015-1639 du 11 décembre 2015.

Les finalités qui pourront être invoquées pour mettre en œuvre ces techniques sont[97] :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale, pour les seuls services du renseignement territorial ;
- la prévention du terrorisme ;
- la prévention :
  - a) des atteintes à la forme républicaine des institutions ;
  - b) des actions tendant au maintien ou à la reconstitution de groupements dissous ;
  - c) des violences collectives de nature à porter gravement atteinte à la paix publique ;
- la prévention de la criminalité et de la délinquance organisées.

La CNCTR constate que la liste des techniques autorisables ainsi que celle des finalités invocables pour les mettre en œuvre sont les mêmes que celles dont les services déconcentrés concernés bénéficient à ce jour, sous l'autorité de leur direction centrale. La création de directions territoriales de la police nationale ne modifie donc pas les compétences des services que ces directions ont vocation à commander de manière unifiée.

Près de quatre ans après l'entrée en vigueur du décret[98] permettant aux services déconcentrés concernés d'être autorisés à mettre en œuvre des techniques de renseignement, aucun élément ne conduit la commission à recommander de restreindre leurs compétences en la matière. La CNCTR n'émet donc pas d'objection au projet de décret sur ce point.

d) Eu égard à l'ensemble des développements qui précèdent, la CNCTR émet un avis favorable au projet de décret qui lui est soumis par le ministre de l'intérieur.

97 - Ces finalités sont celles prévues aux 1°, 4°, 5° et 6° de l'article L. 811-3 du code de la sécurité intérieure.

98 - Voir les dispositions réglementaires du livre VIII du code de la sécurité intérieure, dans leur rédaction résultant du décret n° 2015-1639 du 11 décembre 2015.

Annexe n° 6

Les modifications législatives du livre VIII du code de la sécurité intérieure en 2019

Le tableau ci-dessous résume les modifications de nature législative apportées au livre VIII du code de la sécurité intérieure par l'article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

Loi	Dispositions créées ou modifiées	Objet	Texte d'application
Modifications affectant le régime propre au renseignement pénitentiaire en application duquel le service compétent est autorisé à recourir à certaines techniques de renseignement limitativement énumérées par la loi, aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.			
Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice Voir l'article 89 de la loi (Entrée en vigueur le 25 mars 2019)	Article L. 855-1 du code de la sécurité intérieure (1er alinéa)	**Renforcement des moyens des services du ministère de la justice :** 1. Autorisation de recourir à de nouvelles techniques : - l'interception de sécurité effectuée sur des réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure) ; - la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ; - l'introduction dans un lieu privé, y compris à usage d'habitation, pour y mettre en place, utiliser ou retirer des dispositifs de captation d'images ou de paroles (article L. 853-3 du code de la sécurité intérieure).	

Loi	Dispositions créées ou modifiées	Objet	Texte d'application
Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice Voir l'article 89 de la loi (Entrée en vigueur le 25 mars 2019)	(2ème alinéa)	2. Extension du public susceptible d'être visé par ces services.	
		Limitations nouvelles aux pouvoirs des services du ministère de la justice :	
	(1er alinéa)	1. Limitation du champ d'application de la finalité propre au renseignement pénitentiaire à la prévention des évasions et au maintien de la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.	
	(2ème alinéa)	2. Limitation du champ de la surveillance aux seules personnes qui présentent un risque particulièrement élevé d'évasion ou dont le comportement constitue une menace d'une particulière gravité pour la sécurité au sein des établissements pénitentiaires.	

Loi	Dispositions créées ou modifiées	Objet	Texte d'application
Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice Voir l'article 89 de la loi (Entrée en vigueur le 25 mars 2019)	(2ème alinéa)	3. Limitation aux seules personnes détenues qui présentent un risque particulièrement élevé d'évasion ou dont le comportement constitue une menace d'une particulière gravité pour la sécurité au sein des établissements pénitentiaires, du recours aux techniques de captation d'images ou de paroles dans un lieu privé.	
	(2ème alinéa)	4. Interdiction de surveiller les communications ou les entretiens entre une personne détenue et son avocat.	
	(3ème alinéa)	5. Fixation de contingents limitant le nombre d'autorisations simultanément en vigueur pour les trois techniques mentionnées au point 1.	Décision du Premier ministre en date du 17 juillet 2019



Hôtel de Cassini - 32 rue de Babylone - 75007 Paris